MFN 09-352

Enclosure 2

Licensing Topical Report NEDO-33268, "ESBWR Human Factors Engineering Human-System Interface Design Implementation Plan,"

Revision 4

Non-Proprietary Version

HITACHI

GE Hitachi Nuclear Energy

NEDO-33268
Revision 4
Class I
DRF 0000-0051-1678
May 2009

Licensing Topical Report

ESBWR HUMAN FACTORS ENGINEERING HUMAN-SYSTEM INTERFACE DESIGN IMPLEMENTATION PLAN

PROPRIETARY INFORMATION NOTICE

This is a non-proprietary version of NEDE-33268P, which has the proprietary information removed. Portions of the document that have been removed are indicated by an open and closed bracket as shown here [[ ]].

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT

Please Read Carefully

The information contained in this document is furnished as reference to the NRC Staff for the purpose of obtaining NRC approval of the ESBWR Certification and implementation. The only undertakings of GE Hitachi Nuclear Energy (GEH) with respect to information in this document are contained in contracts between GEH and participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone other than that for which it is intended is not authorized; and with respect to any unauthorized use, GEH makes no representation or warranty, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document.

Table of Contents

List of Tables

List of Figures

SUMMARY OF CHANGES (NEDO 33268, REV 4 VS. REV 3)

Item	Location	Change	Comment
1.	Cover Page	Updated.	N/A
2.	2.1.1 and 2.1.2	Removed or updated references revision levels as appropriate.	N/A
3.	3.1.3 First set of bulleted items	Added second bullet OER/BRR as direct input to HSI design.	As a result of RAI 18.8-51 S02
4.	3.1.3 fifth paragraph and bulleted items	Added Bullet for minimum inventory and revised bullet related to Reg. guide 1.97 to reflect proper title.	As a result of RAI 18.5-27 S03
5.	3.2.3 second paragraph	Added last sentence discussing minimum inventory	As a result of RAI 18.5-27 S03
6.	4.1.2 second paragraph in Operating Experience section	Added clarification that OER provides HSI design requirements.	As a result of RAI 18.8-51 S02
7.	4.2.4 added second Paragraph	Added paragraph to describe specificity and detail of requirements within the style guide	As a result of RAI 18.8-2 S03
8.	4.3.4.6 last paragraph	Added sentence pointing to Appendix B for more detailed test and evaluation work process	As a result of RAI 18.8-35 S04
9.	5.1	Added bullet discussing minimum inventory	As a result of RAI 18.5-27 S03
10.	Figure 2	Added OER/BRR input directly to HSI.	As a result of RAI 18.8-51 S02

SUMMARY OF CHANGES (NEDO 33268, REV 4 VS. REV 3)

Item	Location	Change	Comment
11.	Appendix A	New Appendix provides work process to develop style guide and control room HSIs	As a result of RAI 18.8-2 S03, 18.8-50 S02, 18.8-52 S02, 18.8-53 S01 through 58 S01
12.	Appendix B	New Appendix provides details of testing, evaluation, and trade-off study methods.	As a result of RAI 18.8-35 S04, and 18.8-59 S02

1. OVERVIEW

The Human System Interface (HSI) design process translates functional and task requirements into HSI characteristics, displays, software, and hardware for monitoring, control, and protection functions during normal and accident situations. The HSI is based on the use of a structured methodology that guides designers in identifying and selecting candidate HSI approaches, defining the detailed design, and performing HSI tests and evaluations. It describes the development and use of Human Factors Engineering (HFE) guidelines that are tailored to the unique aspects of the ESBWR design. The plan develops the process by which the ESBWR HSI design requirements are identified, refined, and established. The purpose is to ensure consistency with accepted HFE guidelines, principles, and methods. The result is a safe, simple, and standardized plant design.

This plan systematically delineates the requisite HFE principles necessary to translate functional and task requirements to the design of alarms, displays, controls, and other aspects of the control and instrumentation systems and HSI. Figure 1 shows where this HSI Design Implementation Plan fits into the overall HFE Process.

The HSI design methodology establishes standardization and consistency in applying HFE guidelines, principles, and methods. The process and the rationale for the HSI design are documented and managed under General Electric Hitachi Nuclear Energy (GEH) Quality Assurance (QA) and the ESBWR Man-Machine Interface System (MMIS) and HFE Implementation Plan.

An objective of the HFE program is to resolve issues related to the detailed design of specific aspects of the MMIS during HSI design rather than at HSI Verification and Validation (V&V). Acceptable display formats or alarm system-processing design tradeoffs are established during the HSI design activities through the systematic application of HFE principles.

The Nuclear Regulatory Commission's guidance document NUREG-0700, breaks the HSI into three (3) basic elements:

(1) Information Displays

(2) User-Interface Interaction and Management

(3) Controls

Those elements are delineated into seven (7) system functions, which are:

(1) Alarms

(2) Safety Function and Parameter Monitoring

(3) Group-View Displays

(4) Soft-Controls

(5) Computer-Based Procedures

(6) Computerized Operator Supports

(7) Communication

NRC guidance documents discuss workstation and workplace design as well as HSI support. The ESBWR HSI implementation plan takes into account and uses as practical and appropriate the NUREG guidance that is provided as a baseline HSI plan development.

The HSI Design Implementation Plan establishes:

(1) The methods and criteria for HSI design in accordance with accepted human factors practices and principles

(2) That the HSI design

  a. Implements the information and control requirements developed through the operational analyses, including the displays, controls, and alarms necessary for the execution of those tasks identified in the task analyses as being critical tasks

  b. Defines the basis for a style guide for alarms, displays, and controls as defined the ESBWR operational analyses

(3) The methods for comparing the consistency of the HSI human performance, equipment design, and associated workplace factors with those modeled and evaluated within the completed task analysis (TA)

(4) The HSI design criteria and guidance for control room operations during periods of maintenance and test

(5) The test and evaluation methods for resolving HFE/HSI design issues. These test and evaluation methods include the criteria to be used in selecting HFE/HSI design and evaluation tools

The electronic screen formats, which form a major portion of the HSI are developed in preliminary form as a portion of the HSI part-task simulator and are developed in final format in compliance with the HSI design requirements as part of the entire software development activity.

The HSI design includes features, which facilitate operator activities intended to maintain the operators' vigilance. Features of the HSI are designed using methods that are based upon applicable industry research and publications. The bases for the features, including a review of the experience of selected HSI features are a part of the documented design.

The design of the information and controls located at the operator sit-down workstation are integrated with the design of the mimics displayed on the wide display panel (WDP) for consistency in nomenclature, symbols, and color.

Human factors principles are followed and the color-coding, mimics, labeling, and demarcation are applied consistent with the main control room consoles.

1.1 PURPOSE

This plan develops the process by which the ESBWR HSI design requirements are identified, refined, and established. The purpose is to ensure consistency with accepted HFE guidelines, principles, and methods. The result is a safe, simple, and standardized plant design.

This plan systematically delineates the requisite HFE principles necessary to translate functional and task requirements into the design of alarms, displays, controls, and other aspects of the control and instrumentation systems and HSI. Figure 1 shows where this HSI Design Implementation Plan fits into the overall HFE Process.

1.2 SCOPE

The scope of this HSI Design Implementation Plan establishes:

(1) The methods and criteria for designing the HSI in accordance with accepted human factors guidelines, principles, and methods

(2) HSI information and control requirements

   a. Support critical tasks identified through the operational analyses

   b. Identify the displays, controls, and alarms necessary for the execution of those tasks

   c. Ensure identified plant parameters used for calculation of operational limits are presented as alarms, displays, and controls

   d. Eliminate errors associated with risk-important human actions

   e. Identify error-likely situations

(3) Methods to evaluate the HSI equipment design to support the human performance characteristics established in the TA and the workplace factors under which the operators will perform the associated tasks

(4) HSI design criteria and guidance for operations during periods of maintenance and test

(5) Test and evaluation methods to identify HFE/HSI design issues

(6) Documentation for any human engineering discrepancies (HEDs) as well as strategies for HED resolution

Operational aspects of the HSI process are addressed in the Human Performance Monitoring program, Reference 2.1.2(12). These involve the process for refining and updating the HSI design, including:

- Modifying and updating the HSI
- Making temporary changes to the HSI
- Creating operator defined HSIs (temporary displays defined by operators for monitoring specific plant situations)
- Procedures governing permissible operator initiated changes to HSIs

The scope includes the main control room (MCR), remote shutdown system (RSS) station, and local control stations (LCSs) with a safety-related function or as defined by TA, the Technical Support Center (TSC) and the Emergency Operations Facility (EOF).

1.3 DEFINITIONS AND ACRONYMS

Several terms are defined to provide a common basis for developing training recommendations referred to in this plan.

1.3.1 Definitions

Accident: event that has the potential for release of significant amounts of radioactive material.

Accident Situation: an abnormal plant state occurring during an accident, which may lead to a new damage condition. Operating crews' actions can prevent, mitigate or exacerbate the accident progression.

Action: involves observable movement from one location to another during task performance.

Allocation of Functions (AOF): assignment of responsibility for performing operations required for accomplishing functions to humans, machines, or some combination of both.

Cognitive: the thinking portion of a task, often performed by the control room operators. This involves determining the present condition or state of the plant and the proper recovery action(s) to be performed.

Consequences: the results of (that is, events that follow and depend upon) a specified event.

Control Function: keeping measured functional parameters within bounds though a process of manipulating low-level functions to satisfy a higher-level function (NUREG-0711).

Framework: a systematic organization of tasks or activities used in a specified type of analysis.

Function: an activity or role performed by a human, structure, or automated system to fulfill an objective (System Functional Requirements Analysis Implementation Plan).

Human Error: a mismatch between a performance demand and the human capability to satisfy that demand.

Human Action (HA): a manual response to a cue involving one person to achieve one task or objective. Potentially risk important actions affect equipment or physical systems. Single human actions can be represented as an event in a fault tree or branch point in an event tree.

HFE Issue Tracking System (HFEITS): an electronic database used to document human factors engineering issues that are not resolved through the normal HFE process and engineering discrepancies (HEDs) from the design verification and validation activities. Additionally, the database is used to document the problem resolution.

Human Reliability Analysis (HRA): a structured approach used to identify potential human failure events and to systematically estimate the probability of those errors using data, models, or expert judgment (ASME-RA-S-2002).

(1) **Human-System Interface (HSI):** in general the HSI encompasses all instrumentation and control systems provided as part of the ESBWR for use in performing the monitoring, control, alarming, and protection functions associated with all modes of plant normal operation (i.e., startup, shutdown, standby, at power operation, and refueling) as well as off-normal, emergency, and accident conditions. Specifically, the HSI is the organization of inputs and outputs used by personnel at a location to interact with the plant, including the using of alarms, displays, controls, and job performance aids. Generically, this includes

interfaces that support actions for monitoring, controlling, maintaining protection functions, responding to events, and performing maintenance, calibration, inspection and testing activities. The details of the HSI systems are defined in ESBWR DCD, Tier 2, Chapter 7.

HSI Technology: refers to the types of interfaces that may be available to the operator such as switches, pushbuttons, video displays and associated on-screen controls, crew displays, keyboards, mice, touch screens etc.

Local Control Station (LCS): an operator interface related to process control that is not located in the Main Control Room (MCR). This includes multifunction panels, as well as single-function LCSs such as controls (for example, valves, switches, and breakers) and displays (for example, meters) that are operated or consulted during normal, abnormal, or emergency operations.

Man-machine Interface System (MMIS): the MMIS encompasses all instrumentation and control systems provided as part of the ESBWR which perform the monitoring, control, alarming, and protection functions associated with all modes of plant normal operation (that is, startup, shutdown, standby, power operation, and refueling) as well as off-normal, emergency, and accident conditions.

Maintenance: activities carried out to keep systems and equipment available. Specific types of maintenance include preventive, and corrective. Activities associated with preventive maintenance include testing, surveillance, inspection, and calibration. Activities associated with corrective maintenance include repair, replace, and modify.

Mockup: a static representation of a human-system interface.

Operating Crew: qualified operations staff at the plant during a shift that manages and performs activities necessary to operate the plant and maintain its safety.

Operating Experience Review (OER): a systematic review, analysis and evaluation of operating experience that can apply to the development of the man machine interface design.

Recovery: a general term describing restoration and repair acts required to change the initial or current state of a system or component into a position or condition needed to accomplish a desired function for a given plant state (ASME-RA-S-2002).

Response: to react to a cue for action in initiating or recovering a desired function.

Risk-Important Human Actions: actions performed by plant personnel to provide reasonable assurance of plant safety. Actions may be made up of one or more tasks. There are both absolute and relative criteria for defining risk-important actions. From an absolute standpoint, a risk-important action is any action whose successful performance is needed to provide reasonable assurance that predefined risk criteria are met. From a relative standpoint, the risk-important actions may be defined as those with the greatest risk in comparison to all human actions. The identification can be done quantitatively from risk analysis and qualitatively from various criteria such as task performance concerns based on the consideration of performance shaping factors (NUREG-0711).

Safety Systems: those systems that are designed to prevent or mitigate a design-basis accident (ASME/-RA-S-2002).

Situation Awareness: the relationship between the operator's understanding of the plant's condition, and its actual condition at any given time.

Style Guide: a document that contains tailored guiding principles that describe the implementation of HFE guidance to a specific design, such as for a plant control room. Adherence is expected and deviations justified.

Support System: a system that provides a support function (for example, electric power, control power, or cooling) for one or more other systems (ASME-RA-S-2002).

Task: a collection of activities with a common purpose, often occurring in temporal proximity, with an identifiable start and end point for which human actions are performed using displays and controls.

1.3.2 Acronyms

The following is a list of acronyms used in this plan.

Acronym	Description
ABWR	Advanced Boiling Water Reactor
AEO	Auxiliary Equipment Operator
AOF	Allocation of Function
AOP	Abnormal Operating Procedure
BRR	Baseline Review Record
BWR	Boiling Water Reactor
CA	Corrective Action
CAP	Corrective Action Program
CBP	Computer Based Procedures
CRDT	Control Room Design Team
CTA	Cognitive Task Analysis
D3	Defense-in-Depth and Diversity
DCD	Design Control Document
EID	Ecological Interface Design
EOC	Extent-of-Condition
EOF	Emergency Operations Facility
EOP	Emergency Operating Procedures
EPG	Emergency Procedure Guidelines
ERP	Eye Reference Point
FRA	Functional Requirements Analysis
FSS	Full Scope Simulator

GEH	General Electric Hitachi Nuclear Energy
GUI	Graphical User Interface
HA	Human Actions
HED	Human Engineering Discrepancy
HFE	Human Factors Engineering
HFEITS	Human Factors Engineering Issue Tracking System
HPES	Human Performance Evaluation System
HPM	Human Performance Monitoring
HPMIP	Human Performance Monitoring Implementation Plan
HRA	Human Reliability Analysis
HSI	Human-System Interface
LCS	Local Control Station
MCR	Main Control Room
MMIS	Man-Machine Interface Systems
N-DCIS	Nonsafety-Related Distributed Control and Information System
NPP	Nuclear Power Plant
OER	Operating Experience Review
PAS	Plant Automation System
PFRA	Plant-Level Functional Requirements Analysis
PRA	Probabilistic Risk Assessment
PRA/HRA	Probabilistic Risk Assessment / Human Reliability Assessment
QA	Quality Assurance
Q-DCIS	Safety-Related Distributed Control and Information System
RSR	Results Summary Report
RSS	Remote Shutdown System
RWCU	Reactor Water Cleanup
S&Q	Staffing and Qualifications
SAMG	Severe Accident Mitigation Guidelines
SDC	Shutdown Cooling
SDS	System Design Specifications
SFRA	System Functional Requirements Analysis
SME	Subject Matter Expert

SPDS	Safety Parameter Display System
SSC	Systems, Structures, and Components
TA	Task Analysis
TMI	Three Mile Island
TSC	Technical Support Center
WDP	Wide Display Panel
V&V	Verification and Validation
VDU	Video Display Unit

2. APPLICABLE DOCUMENTS

Applicable documents include supporting documents, supplemental documents, codes and standards, and are given in this section. Supporting documents provide the input requirements to this plan. Supplemental documents are used in conjunction with this plan. Codes and standards are applicable to this plan to the extent specified herein.

2.1 SUPPORTING AND SUPPLEMENTAL GEH DOCUMENTS

2.1.1 Supporting Documents

The following supporting documents were used as the controlling documents in the production of this plan. These documents form the design basis traceability for the requirements outlined in this plan.

(1) ESBWR DCD, Chapter 7, (GE 26A6642AW)

(2) ESBWR DCD, Chapter 18, (GE 26A6642BX)

(3) NEDE-33217P and NEDO-33217, Rev. 5, "ESBWR Man-Machine Interface System And HFE Implementation Plan"

2.1.2 Supplemental Documents

The following supplemental documents are used in conjunction with this document plan.

(1) NEDO-33219, Rev. 3, "ESBWR HFE Functional Requirements Analysis Implementation Plan"

(2) NEDE-33220P and NEDO-33220, Rev. 3, "ESBWR HFE Allocation of Function Implementation Plan"

(3) NEDO-33221, Rev. 2, "ESBWR HFE Task Analysis Implementation Plan"

(4) NEDO-33251 Rev. 1, "ESBWR I&C Diversity and Defense-In-Depth Report"

(5) NEDO-33262, Rev. 2, "ESBWR HFE Operating Experience Review Implementation Plan"

(6) NEDO-33266, Rev. 2, "ESBWR HFE Staffing and Qualifications Implementation Plan"

(7) NEDO-33267, Rev. 3, "ESBWR HFE Human Reliability Analysis Implementation Plan"

(8) NEDO-33274, Rev. 3, "ESBWR HFE Procedures Development Implementation Plan"

(9) NEDO-33275, Rev. 3, "ESBWR HFE Training Development Implementation Plan"

(10) NEDE-33276P, and NEDO-33276, Rev. 2, "ESBWR HFE Verification and Validation Implementation Plan"

(11) NEDO-33277, Rev. 3, "ESBWR HFE Human Performance Monitoring Implementation Plan"

(12) NEDO-33278, Rev. 3, "ESBWR HFE Design Implementation Plan"

2.2 CODES AND STANDARDS

The following codes and standards are applicable to the HFE program to the extent specified herein.

(1) IEEE Std. 497, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," 2002

(2) IEEE Std. 1023, "Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating stations", 2004

(3) ASME-RA-S, Standard for Probabilistic Risk Assessment For Nuclear Power Plant Applications, 2002.

2.3 REGULATORY GUIDELINES

(1) NUREG-0696, "Functional Criteria for Emergency Response Facilities", 1980

(2) NUREG-0700, Rev. 2 "Human System Interface Design Review Guideline"

(3) NUREG-0711, Rev. 2 "Human Factors Engineering Program Review Model"

(4) NUREG-0737, Supplement 1, "Requirements for Emergency Response Capability", 1980

(5) NUREG-0835, "Human Factors Acceptance Criteria for the Safety Parameter Display System", 1983

(6) NUREG-1342, "A Status Report Regarding Industry Implementation of Safety Parameter Display System", 1989

(7) Regulatory Guide 1.105, "Setpoints for Safety-Related Instrumentation", December, 1999

(8) Regulatory Guide 1.206, "Combined License Application for Nuclear Power Plants (LWR Edition)", C.I.18, Human Factors Engineering, June 20, 2007

(9) Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions", February 1972

(10) Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Systems", May 1973

(11) Regulatory Guide 1.62, "Manual Initiation of Protective Actions", October 1973

(12) Regulatory Guide 1.97, Rev. 4, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants", June 2006

2.4 DOD AND DOE DOCUMENTS

None.

2.5 INDUSTRY AND OTHER DOCUMENTS

None.

3. METHODS

This document meets the following objectives:

(1) Describes the HSI design process

(2) Presents the HSI Implementation Plan and the proposed HSI style guide that is used to execute the design process

(3) Provides guidance to the HSI design team members to understand their roles and direct their design activities

(4) Provides illustration to regulatory authorities that the new HSI is designed following the process guidance found in the respective industry documents

(5) Means to select technology for design application (presented in the HSI style guide)

3.1 CONCEPT DESIGN

The HFE team uses several approaches for developing a concept design as described in NUREG-0711. The operational analysis (including development of a functional requirement specification), modification of predecessor designs, surveys of the state-of-the-art in HSI technologies, and predecessor and ABWR reference designs contribute significantly to HSI development. Human performance issues identified from previous operating experience with the predecessor designs are resolved in the conceptual design.

Evaluation of the conceptual design includes comparison with operating experience and literature analyses, tradeoff studies, engineering evaluations, and experiments. Alternative concept designs are considered for elements of the HSI. Evaluations provide reasonable assurance that the selection process is based on a thorough review of design characteristics and a systematic application of selection criteria. Tradeoff analyses, based on the selection criteria, provide a rational basis for the selection of concept designs. HSI design performance requirements are identified for components of the selected HSI concept design. These requirements are based on the functional requirement specifications but are refined to reflect HSI technology considerations identified in the survey of the state of the art in HSI technologies and human performance considerations identified in the human performance research.

3.1.1 Background

Revision 2 of NUREG-0700 provides the base guidance for the ESBWR HSI design process. NUREG-0700 was first published (Revision 0) in 1981 as a response to the Three Mile Island (TMI) accident. Following TMI, all U.S. nuclear power plants were required to conduct detailed control room design reviews Detailed Control Room Design Review, including review of remote shutdown panels, to identify and correct human factors design deficiencies. NUREG-0700, Revision 0, provided extensive guidelines to support those reviews. Revision 1 to NUREG-0700, published in June 1996, updated the guidance to address the emergence of advanced HSI technologies into nuclear power plant design. Revision 2, published in May 2002, expanded the guideline information in the following areas:

(1) HSI design process

(2) Information display

(3) User interface interaction and management

(4) Process control and input devices

(5) Alarm systems

(6) Safety Function and Parameter Monitoring

(7) Group-View Display System

(8) Soft Control System

(9) Computer-Based Procedure System

(10) Computerized Operator Support system

(11) Communication System

(12) Workstation Design

(13) Workplace design

(14) Maintainability of Digital Systems

Identification of the HFE/HSI issues is performed through document review and personnel surveys in the OER activity. The ESBWR OER identifies and analyzes HFE/HSI-related issues encountered in plant operating history and in the general nuclear power industry so that they are avoided in the development of the new HSI design.

The OER encompasses the following aspects:

(1) Document review

(2) Plant personnel (MCR operator) surveys

(3) HFE issues analysis and documentation

(4) Completion and analysis of questionnaire identifying positive features of existing HSI

Allocation of function (AOF) is defined as the "analysis of the requirements for plant control and the assignment of control functions to:

(1) Personnel (for example, manual control)

(2) System elements (for example, automatic control and passive, self-controlling phenomena)

(3) Combinations of personnel and system elements (for example, shared control and automatic systems with manual backup)"

The AOF is an HFE process that is used to determine the level of automation for a system. The AOF process exploits the strengths of personnel and system elements. It is based on HFE principles using a structured and well-documented methodology that seeks to provide plant operators with logical, coherent, and meaningful tasks.

AOF is not based solely on technology considerations that allocate to plant personnel everything the designers cannot automate. Such an approach results in activities that are likely to negatively affect operator performance. The design does not embrace automation for the sake of automation, but rather selectively automates in order to maintain operator situational awareness and vigilance.

The AOF report describes the approach to determining AOF and presents the results for safety functions. A top-down approach is used to develop the AOF decisions.

For each system identified in the functional requirements analysis (FRA), the AOF methodology is applied and a level of automation is specified and documented. The result summary report (RSR) includes a specification of the current level of automation and personnel responsibility for safety functions, and the associated safety-related processes and systems. The rationale for the current plant AOF decisions, pertaining to the ESBWR safety functions, is also documented.

The AOF RSR also includes a description of HFE activities that are conducted as part of the HSI design process to verify the adequacy of current AOF decisions, and establishes the capability of operators to perform the role assigned to them. This includes:

- How human factors input is provided early in the design process
- How the role of the operator is considered in assigning AOF
- Mechanisms available for reconsidering, and if necessary, changing AOF in response to operating experience and the outcomes of ongoing analyses and trade-off studies

While this initial AOF documents the current level of automation (and the rationale) for systems affecting the safety systems, the AOF is revised, if needed, following completion of the OER/Baseline Review Record (BRR) report. If, after considering OER/BRR results, an AOF decision changes the current level of automation (function allocation) and the respective system is part of the decomposition of one of the critical safety functions (FRA), then the AOF documentation is revised.

3.1.2 Goals

The primary goal for HSI designs is to facilitate safe, efficient and reliable operator performance during all phases of normal plant operation, abnormal events and accident conditions. Maintenance, test, and inspection activities are also considered. To achieve the operator performance goals, information, displays, controls, and other interface devices in the control room and other plant areas are designed and implemented in a manner consistent with good HFE practices. The goals can be summarized as fulfilling the following:

- Maximize plant capacity/output power levels
- Achieve and maintain high reliability
- Achieve and maintain high availability
- Maintain high levels of safety
- Maintain high levels of operator awareness of the plant and equipment states
- Minimize the likelihood of human errors
- Integrate fault tolerance and fault recovery into the systems (both from potential human and equipment errors)

The objective of the HSI concept design process is to produce an HSI design that presents plant information and controls in a useful, effective, and operator-friendly manner and allows the operators to safely monitor and control the plant under all operating conditions. A well-defined design process that incorporates industry-accepted HFE principles is used to achieve this objective.

3.1.3 Basis and Requirements

The HFE team develops functional requirements for the HSI to address the concept of operations. The requirements are based on the:

- Personnel functions and tasks defined in the operations analysis
- OER/BRR
- S&Q analysis
- Requirements for a safe, comfortable working environment

The HSI requirements address the various types of HSIs, for example, alarms, displays, and controls.

The three components of HSI design, concept design, style guide, and detailed design share similar bases and requirements.

The concept design uses human factor elements, as defined in the DCD Chapter 18 and the MMIS and HFE Implementation Plan, to address HFE issues during the HSI design process. The HSI design, hardware, software, logic, controls, indications and the style guide that governs their creation conform to the principles set forth in regulations including:

- NUREG-0700
- NUREG-0711
- Reg. Guide 1.206, Section C.I.18

In addition, the HSI design for the control room and applicable facilities addresses the guidance for the following seven key aspects of the plant HSI:

- The minimum inventory of alarms, displays, and controls presented in DCD Table 18.1-1a and Table 18.1-1b are included in the designs of the MCR and RSS, respectively.
- Provision for periodic testing of protection systems actuation functions, as described in Regulatory Guide 1.22
- Bypassed and inoperable status indication for NPP safety systems, as described in Regulatory Guide 1.47
- Manual initiation of protective actions, as described in Regulatory Guide 1.62
- Accident monitoring instrumentation for nuclear power plants, as described in Regulatory Guide 1.97
- Instrumentation setpoints, as described in Regulatory Guide 1.105
- HSIs for the emergency response facilities (TSC & EOF), as described in NUREG-0696

The HFE design team reviews and verifies that the HSI concept design uses accepted HFE principles in its form and presentation of information and in its interactions with plant personnel.

Additionally, the Computer Based Procedures (CBPs) presented by the HSI conform to the principles set forth in NUREG-0700.

3.1.4 General Approach

Due to increasing regulatory and utility requirements, and demands for greater plant availability, it is necessary to incorporate innovative designs reflecting advances in computer-based technology. In recent years, the major nuclear plant vendors have been developing control complexes that make use of computers to process plant parameter data and display information to personnel. Computer based applications reduce the number of hardwired instruments needed to provide information about plant operations. In addition, computer-aiding routines are incorporated to unburden plant personnel, thereby allowing them to direct their attention to monitoring, and analysis and decisions regarding plant operations.

Figure 1 outlines the overall flow of the HFE process and the portions of the process that provide input to HSI design. Processes that receive input from HSI design are also shown. The primary input to HSI design is data processed through operational analysis. Operational analysis receives input from:

- HRA/PRA results and risk significance determinations
- OER/BRR results and lessons learned
- Defense-in-Depth and Diversity (D3) (Reference 2.1.2(4))
- Design Control Document (DCD) specifications and requirements
- System Design Specifications (SDS)

These inputs are processed through design, detailed, and economic analyses in the FRA, AOF, and TA phases of the operational analysis. Outputs from TA form the inputs to HSI design. Operational analysis provides or refines:

- Requirements to the HSI Implementation Plan
- Detailed procedure outlines to the Procedure Development Plan
- Task sequence and interlock logic for plant automation and auto control of functions

Operational analysis identifies the individual mental and physical tasks necessary to support the functions allocated to humans, machine, or shared.

The Staffing and Qualification (S&Q) process provides additional input to HSI Design that when combined with operational analysis specifications in accordance with the HSI style guide generate HSI specifications.

Feedback inputs to the HSI design process are through the operational analysis process and include issues and lessons learned impacting HSI design from:

- Training program
- Procedure program
- Validation and Verification (V&V)
- Human Performance Monitoring (HPM)

- HFEITS

Figure 2 outlines the flow of information and processes within the HSI design process. The first step in this process is the HSI concept design, which lays out the overall framework from which the ESBWR style guide and the detailed HSI design are developed and refined.

A summary of the HSI design process is presented in the following steps:

Step 1: Workspace and Environmental Conditions Design

The external MCR and RSS stations display features are defined including general layout, fields of vision, access and egress, seating, procedure lay down areas, general anthropometric dimensions, and environmental temperature/humidity expectations.

Step 2: Panel Layout Design

The components mounted on the MCR and RSS stations panels and console, and their organization and arrangement are defined.

Step 3: Alarm System Design

The alarm system is defined including conceptual display hierarchy, presentation, and layout.

Step 4: Displays and Control Design

The information and control requirements derived from the operational analysis and other inputs are implemented into the MCR and RSS components.

Step 5: Communication System Design

Design aspects of a communication system are defined.

3.1.5 Application

A most critical question for the behavioral specialist is: For whom is the user and/or operator of the system to be designed? More important, what is this human supposed to do? The behavioral specialist is aware of the physical functions to be performed by the system (because these determine the behavioral functions the human performs), but the primary concern is the derivation of behavioral functions from physical ones.

For example, if a display is presented to the operator of a system, the behavioral functions of monitoring, analyzing, and interpreting are inevitably involved. The more information provided by the technology, the more detailed is the derivation of the human function/sub function. If the designer of an interface merely says a display is provided, the specialist can deduce only that perceptual-cognitive activity is required. If the designer says that the display is a multivariate display reporting the interactions of multiple dimensions (level, pressure, temperature, etc.), the specialist is able to decompose the perceptual-cognitive function into more meaningful sub functions.

The conceptual design portion of the overall HSI design process analyzes the basic HSI requirements generated in operational analysis and the human factors insight gained from HFE specialists and generates the HSI conceptual design. The conceptual design meets the process goals by satisfying the HSI design requirements in a manner that takes advantage of human strengths while avoiding human weaknesses.

3.2 HSI SPECIFIC GUIDANCE – STYLE GUIDE

The purpose of the HSI style guide is to provide a set of HSI design guidelines to be used by the HSI designers to help ensure that a consistent design philosophy is applied. As suggested throughout NUREG-0700, ESBWR implementation guidelines are developed by tailoring the guidance provided by NUREG-0700 to the ESBWR specific applications. Deviations from NUREG 0700, if any, will be justified. The resulting HSI implementation guidelines include the following:

(1) Anthropometric and ergonomic design guidelines

(2) HSI display format philosophy

(3) Display implementation guidelines

The anthropometric data include 5th percentile female and 95th percentile male data from the United States populations for measures such as arm length, sitting eye height, functional reach, etc. This helps designers produce guidelines for physical clearances and reach envelopes. Employing these guidelines ensures that objects in the control room do not impede operator actions, and that a wide range of operators is accommodated.

Ambient and direct lighting, glare, and viewing distance guidelines are noted to provide sufficient readability of all text-based and color-coded items in the control room.

Auditory thresholds and guidelines are outlined so alarms and auditory signals are designed for maximum operator detection.

Guidelines for environmental factors such as temperature, humidity, and radiation exposure are addressed to provide comfort and safety for the operators in the control room at all times.

The HSI style guide document establishes requirements for the display formats made available to the operators. The HSI style guide includes descriptions of display hierarchy, presentation, and navigation.

The HSI style guide also defines a set of standards (e.g., general layout, text size, usage of colors, symbols, static/dynamic elements, etc.) that are followed by multiple display designers to ensure consistency when creating the various display formats for the ESBWR project. The guidelines for the conventional HSI are also included in the HSI style guide.

Figure 2 illustrates the inputs used to develop the HSI implementation guidelines and the relationship of these guidelines to the HSI design effort. The HSI implementation guidelines are used along with the HSI conceptual design documentation to develop the HSI design specifications.

3.2.1 Background

The following sources of information provide input to the HSI design process:

(1) Analysis of Personnel Task Requirements - The analyses performed in earlier stages of the design process are used to identify requirements for the HSI. These analyses include:

   a. Operational Experience Review - Lessons learned from other complex human-machine systems, including ABWR reference designs and designs involving similar HSI technology are used as an input to HSI design

b. FRA and AOF - The HSI supports the operator's role in the plant, for example, appropriate levels of automation and manual control

c. TA - The set of requirements to support the role of personnel is provided by TA. The TA identifies:

   i. Tasks that are necessary to control the plant in a range of operating conditions for normal, abnormal, and accident conditions

   ii. Detailed information and control requirements (for example, requirements for display range, precision, accuracy, and units of measurement)

   iii. Task support requirements (for example, special lighting and ventilation requirements)

   iv. Risk-important HAs and their associated performance shaping factors, as identified through HRA are given special attention in the HSI design process

d. S&Q - The results of S&Q analyses provide input for the layout of the overall control room and the allocation of controls and displays to individual consoles, panels, and workstations. They establish the basis for the minimum and maximum number of personnel to be accommodated and requirements for coordinating activities between personnel.

(2) System Requirements - Constraints imposed by the overall I&C system are considered throughout the HSI design process

(3) Regulatory Requirements - Applicable regulatory requirements are identified as inputs to the HSI design process

As the design progresses the HFE team identifies other requirements that become inputs to the HSI design.

3.2.2 Goals

The style guide defines the HSI structure, layout, color schemes, screen hierarchy, and hardware options from which the HSI is designed and developed. It also provides direction regarding how the criteria are to be applied. Compliance with style guide criteria when designing the HSI to meet the requirements set forth by operational analysis ensures the following goals are met:

- Standardization
- Consistency
- Uniformity
- Relevancy of meaning
- Discrimination of alarms and states
- Accommodation of user expectations
- Navigability
- Compliance with good HFE practices

- Minimize human error

3.2.3 Basis and Requirements

The design uses human factor elements, as defined in the DCD Chapter 18 and the MMIS and HFE Implementation Plan, to address HFE issues during the HSI design process. The HSI design, hardware, software, logic, controls, indications and the style guide that governs their creation conform to the principles set forth in regulations including:

- NUREG-0700
- NUREG-0711
- Reg Guide 1.206, Section C.I.18

Design considerations relative to NUREG-0711 referenced Regulatory Guides are considered in the HSI design process. These include consideration for control room functions that provide for periodic testing (RG 1.22), display status of bypassed or inoperative safety system indications (RG 1.47), switches or controls required for manual initiation of protective actions (RG 1.62), and aspects of Safety Parameter Display System (SPDS) and continuous display parameters (RG 1.97). Specific requirements and applications result from the functional requirements and tasks analyses. The minimum inventory of alarms, displays, and controls presented in the DCD Table 18.1-1a and Table 18.1-1b are also considered and included in the designs of the MCR and RSS, respectively.

The HFE design team reviews and verifies that the HSI design uses accepted HFE principles in its form and presentation of information and in its interactions with plant personnel. Additionally, the CBPs presented by the HSI conform to the principles set forth in NUREG-0700. The style HSI guide generated in this portion of the process presents design options for use in the ESBWR and the requirements for use and presentation of the HSI elements and CBPs. The HFE design team uses the style guide to properly combine and structure the HSI design elements and operational analysis requirements.

3.2.4 General Approach

The ESBWR HSI style guide is both a product of the HSI design effort and a governing input to it. The style guide is one of the first products generated by the HSI design team. The style guide will be created using input from similar guides from previous designs such as the ABWR, HSI style guides from other industries, NUREG-0700, and other applicable documents. The HSI style guide is a compilation of HSI equipment, control, display, interface, and structures from which designers can select the most appropriate option for a given application. Additionally, the style guide sets requirements for when and how to incorporate the various hardware options.

Similar guidance is provided in the area of HSI software including workstation design and presentation content, format, and logic. Style guide requirements maintain consistency in presentation, navigation, and interface mechanisms between various portions of the HSI. Because human factors criteria and best practices are infused in the style guide requirements, its use ensures HSI design minimizes the likelihood of human error.

3.2.5 Application

Having better theories of users and task domains allows building more usable human-computer interfaces, but it is important to realize that the ultimate usability of a system in a given environment is governed as much by the organization of work around the system as it is by fundamental characteristics of the technology itself.

Although the technology does not determine the work organization, it can bias things so that certain kinds of procedures are more likely to be adopted than others. It is at this level that designers can influence how work gets done. This argues for a more thorough analysis of the operating philosophy beyond traditional TA and examining the social and organizational context that influences the operation of work activities. Restricting a person to abstract work procedures and designing systems at this level can lead to unworkable systems.

Insight gained in this area is infused in the criteria contained in the ESBWR HSI style guide. This ensures that HFE goals are met when the technical requirements defined in operational analysis are incorporated into the HSI design in accordance with the style guide.

3.3 HSI DETAILED DESIGN AND INTEGRATION

The detailed design incorporates all of the goals, attributes, and criteria already presented in the conceptual design and style guide discussions above. The detailed design refines and enhances the framework conceptual design. The comprehensive HSI design is created by integrating the broad system designs from the conceptual design effort and supporting details including:

- Alarm hierarchy and detailed presentation requirements
- System mimic displays and presentation requirements including:
  - Color schemes
  - Equipment symbols
  - Data requirements, presentation, sampling and update rates
  - Linked supporting information pages
  - Trending and recording
  - Interfaces and display of linked programs such as clearances
- Integrated plant displays and presentation requirements (similar to system mimics above) including those incorporating SPDS requirements
- Computer based procedure requirements including standard displays, linked automations, linked trending, imbedded controls, procedure place-keeping, etc.
- Plant control displays, standards, and requirements for linked automations, trend graphing, etc.
- Incorporation of, or providing links to, supporting software based administrative programs such as:
  - LCO tracking
  - Clearance process

  - Operator log keeping
  - Work management program
  - Risk evaluation/management program
  - Electronic permanent records storage program
- HSI feedback mechanisms including:
  - Prompts
  - Audible or visual queues
  - Alarms
  - Error messages

3.3.1 Background

The principal objectives of the HSI design are to provide the indications and displays necessary to provide the operator with accurate, complete, and timely information regarding the functional status of plant equipment and systems. HSI also provides control capability to both the plant and the operator. An additional objective of the HSI design is to permit plant commissioning to take place effectively and to permit timely installation, modifications, and maintenance of the HSI.

The ESBWR D3 design (Reference 2.1.2(4)) ensures that the requirements for functional isolation are met. Functional isolation and physical separation are integrated into the design where redundant safety divisions, or safety systems and non-safety systems are brought into close proximity.

The control room provides an environment where tasks are performed without discomfort, excessive stress, or physical hazard. In accordance with habitability requirements, appropriate measures are taken to safeguard the occupants of the control room against potential hazards such as unauthorized access, undue radiation resulting from an accident condition, toxic gases, and consequences of fire, which could jeopardize necessary operator actions.

The HSI basic design is standardized with desired HSI features that enhance the ability of operators to carry out monitoring, planning and response tasks. In order to minimize event initiators HSI design facilitates:

- Normal operations
- Abnormal operations
- Emergency operations
- Maintenance activities

HSI inputs include:

(1) Regulatory guidance

(2) Operating Experience Review (OER) / Baseline Record Review (BRR)

(3) Human Reliability Analysis (HRA) / Probabilistic Risk Assessment (PRA)

(4) Operational analysis requirements from:
   a. Plant and System Functional Requirements Analysis (PFRA and SFRA)
   b. Allocation Of Functions (AOF)
   c. Task Analysis (TA)

(5) Staffing and Qualification (S&Q) requirements

(6) Training

(7) Procedures

(8) Feedback input from Human Performance Monitoring (HPM) and Validation and Verification (V&V)

These design inputs are translated into hardware and software design requirements. These requirements are included in the applicable specifications as well as in the hardware drawings and software programs. Central to this plan is the generation of both a concept design and style guide, both of which input into and govern the development of the detailed design.

In order to evaluate these requirements (for example, operator time critical and reliability critical requirements), studies and tests are performed as necessary. Mockups and models are constructed and/or dynamic simulations performed as necessary to validate the designs.

Figure 2 defines the overall design process described in this plan. In this figure, the expected inputs and outputs are identified. The relationship between this plan and other implementation plans is also identified in Figure 2.

3.3.2 Goals

The primary goal for HSI designs is to facilitate safe, efficient and reliable operator performance during normal, abnormal, and emergency operating conditions. Maintenance, test, and inspection activities are also considered. To achieve this goal, information displays, controls, and other interface devices are designed and implemented in a manner consistent with good HFE practices.

HSI goals can be summarized as:

- Maximizing plant capacity/output power levels
- Achieving and maintaining high reliability
- Achieving and maintaining high availability
- Maintaining high levels of safety
- Maintaining high levels of operator plant and equipment awareness
- Minimizing the likelihood of human errors
- Integrating fault tolerance and fault recovery into systems (both from potential human and equipment errors)

3.3.3 Basis and Requirements

The bases and requirements of the HSI detailed design are similar to the previous two elements. The detailed design uses human factor elements, as defined in the DCD Chapter 18 and the MMIS and HFE Implementation Plan, to address HFE issues during the HSI design process. The HSI design, hardware, software, logic, controls, indications and the style guide that governs their creation conform to the principles set forth in regulations including:

- NUREG-0700
- NUREG-0711
- Reg Guide 1.206, Section C.I.18

The HFE design team reviews and verifies that the HSI detailed design uses accepted HFE principles in its form and presentation of information and in its interactions with plant personnel. Additionally, the CBPs presented by the HSI conform to the principles set forth in and NUREG-0700. Detailed design including software and hardware elements are generated in accordance with the style guide.

3.3.4 General Approach

Specific HFE design guidance is developed using operational analysis requirements and the HFE principles incorporated into the style guide. This guidance is used in the design of the HSI features, layout, and environment.

The HSI detailed design supports personnel in their primary role of monitoring and controlling the plant while minimizing personnel demands associated with use of the displays (for example, window manipulation, display selection, display system navigation). High-level HSI design review principles reflect NUREG-0700 guidelines.

For risk-important Human Actions (HAs), the design seeks to minimize the probability that errors occur and maximize the probability of error detection.

When developing detailed HSI design requirements for monitoring and control capabilities provided either in the control room or locally in the plant, the following factors are considered:

a. Communication, coordination, and workload
b. User feedback
c. Local environment
d. Inspection, test, and maintenance
e. Risk-important elements

The layout of HSI within consoles, panels, and workstations is based upon:

a. Analyses of operator roles (job analysis)
b. Systematic strategies for organization such as arrangement by importance, frequency of use, and sequence of use
c. Accommodation of D3 design (Reference 2.1.2(4))

HSI design supports personnel and task performance during minimal, nominal, and high-level staffing.

The design process addresses the use of the HSIs over the duration of a shift where decrements in performance due to fatigue may be a concern.

HSI characteristics support human performance under the full range of both normal and credible, extreme environmental conditions.

The main control room requirements address conditions such as loss of lighting, loss of ventilation, and evacuation.

The remote shutdown facilities and local control stations requirements address constraints imposed by the ambient environment (for example, noise, temperature, contamination) and by protective clothing (if necessary).

HSIs are designed to support inspection, maintenance, test, and repair of (a) plant equipment and (b) the MMIS. HSIs are designed so that inspections, maintenance, test, and repair of the MMIS does not interfere with other plant control activities.

Modifications to predecessor HSI designs to be used for ESBWR applications are reviewed to address the following considerations.

a. As practical, maintain consistency with user's existing strategies for gathering and processing information and executing actions in the TA

b. As practical, maintain or improve existing support for crew coordination through shared view of plant information and, awareness of others actions and crew communications

c. Developments of design requirements to assure that the relationship among plant systems are consistent with original design, if the modification changes the degree of integration between plant systems

3.3.5 Application

A major aspect of the endpoint vision of the control room is the determination of the capability/functionality of the systems and interfaces. In the past, nuclear power plants had commonly looked at "like-for-like" replacements when defining the modernization of old systems. That is, the plants just implement the same functionality and capability of the old system with new technology. At the most, some simple interface or other minor changes were made. This may be the best modernization solution in some cases. However, in most cases it is not. Therefore, it is important to look at and take advantage of the improvements that modern, digital technology can bring now and in the future. To accomplish this HSI design addresses the following attributes discussed in detail below.

3.3.5.1 *Control Room Interfaces*

Standard Design Features

Using requirements from the ESBWR DCD, results of the operations analysis (PFRA, SFRA, AOF and TA), and the operating experience of BWRs and ABWRs, as part of the design development a program is planned for the purpose of "studying the application of man-machine technologies to enhance the efficiency of operational control of NPPs". A variety of tests, studies, and evaluations are performed in a number of areas of control room equipment design. These studies and evaluations culminate in the fabrication and testing of prototype control room HSI equipment designs.

The HSI design program includes:

(1) Consideration of existing control room operating experience

(2) Review of trends in control room designs and existing control room data presentation methods

(3) Evaluation of new HSI technologies, alarm reduction and presentation methods

(4) Adoption of successful HSI technologies from highly hazardous process control industry, military, and other complex system advances

(5) Review of operations analyses

(6) Validation testing of the prototype. The prototype is evaluated in accordance with the methods and criteria defined in this plan and the Human Factors V&V Implementation Plan.

Following the completion of the prototype tests and implementation of their results, the detailed control room HSI standard design features are finalized.

Location and Protection

Location

The MMIS related to HSI is located where it is not affected by the consequences of plant internal hazards such as missile, radiation, fire, etc., and where operators can easily gain access under all the plant conditions, yet evacuate from the location if the location becomes uninhabitable.

Protection

The design of the MMIS provides, within the design basis, protection against fire, radiation, internal and external missiles, earthquake, and appropriate security measures to control access to HSI software.

(1) Fire Protection

Attention is given to using nonflammable materials in the HSI. The HSI area in the MCR is equipped with fire detection and fire suppression systems.

Electrical equipment in the HSI is designed to neither cause nor support a fire as far as this is reasonably achievable. Cable circuits and switchgear associated with the HSI are protected against the consequences of fire. Cable insulation and sheathing materials are fire-retardant and consistent with applicable national codes for flame propagation, release of combustion products and materials where applicable.

(2) Radiation Protection

The staff is protected against direct radiation in any accident situation. The control room is designed in accordance with applicable codes, standards, and regulatory requirements for habitability.

(3) Missile Protection

The HSI design includes assessment and protection against missiles.

(4) Earthquake Protection

The HSI equipment related to safety functions, the air-conditioning system, and emergency illumination systems are designed in accordance with the applicable codes and standards for postulated design events.

(5) Security

The HSI is designed to allow for control of access to plant system control and databases. Access to the MCR is in accordance with the site security plan.

3.3.5.2 *Human Centered Design*

Realization of a human-centered design requires an understanding of the method of decision-making of a human operator. ESBWR HFE design team has modified an operator decision-making model to clearly define the role of feedback in the decision-making process.

The model identifies four major cognitive activities supported by the HSI:

- Detection and monitoring/situation awareness
- Interpretation and planning
- Control
- Feedback

The HSI resources are designed to promote not only rule-based reasoning by the operators but also knowledge-based reasoning. MCR operators are required to follow procedures while executing plant maneuvers and plant and equipment state changes. The HSI is designed to promote the efficient execution of plant procedures (rule-based reasoning). HSI resources are also designed to promote knowledge-based reasoning. Knowledge-based reasoning is defined as human decision-making based upon their knowledge, training, and plant experience.

Detection and Monitoring/Situation Awareness

Operators monitor plant parameters to understand the plant state. The model is defined broadly to address detection and monitoring during each plant condition. It includes active monitoring guided by procedures or a supervisor, and passive monitoring, such as board scanning. It also includes monitoring to support awareness of the goals and activities of other agents, both people and machines.

Interpretation and Planning

The most critical components of decision-making are correct situation assessment and identification of the most appropriate response plan (procedure), given the current state of the plant.

The need for coordination in carrying out procedures is not explicit in the performance model. The process of initial allocation to human and automated sources, and later coordination of tasks (goals to be addressed) is included in the interpretation and planning area of the model. The HSI model makes explicit the monitoring of goal achievement, which is a means to assess how well each operator or automated system is progressing in achieving goals.

Control

Control involves decisions in the initiation, tuning, and termination of plant processes. Control is simpler for operators when they control the pace of an event. Control becomes more difficult when multiple individuals or autonomous systems must be coordinated to execute a task. While the control area of the model does not explicitly call out the process of locating the controls, it is considered to be part of this area of the model.

Feedback

Feedback occurs at several levels. Initially, operators need to verify that the control is executed by verifying that the plant components have changed state as expected. Second, operators need to monitor the state of plant parameters and processes to determine whether the actions are having the intended effect. The final, and most critical, level of feedback is an evaluation of whether the operational goal is achieved.

3.3.5.3 *Automation Design*

The ESBWR incorporates selected automation of the operations required during normal plant startup/shutdown and during normal power range maneuvers.

The Plant Automation System (PAS) is the primary ESBWR system for providing the automation features for normal ESBWR plant operations while ensuring that ultimate control of the plant remains with the operator.

(1) Automated Operation

During transitions between plant operation modes, the PAS, when in automatic operation, performs sequences of automated plant control operations by sending system or component state change commands and setpoint changes to lower level, nonsafety-related plant system controllers. The PAS cannot directly change the status of a safety-related system. When a change in the status of a safety-related system is required to complete the selected operation sequence, the PAS provides prompts to guide the operator in manually performing the change using the appropriate safety-related HSI controls provided on the main control console.

Automatic actuations such as design basis safety-related automatic actuations or isolations cannot be prevented by normal human actions unless an engineered inhibit or bypass is provided (EOPs and/or SAMGs provide for additional emergency inhibits, and bypasses). Plant automations designed to assist human operation of the plant are provided with alternate human performance and/or human override capability where operational analysis indicates such capabilities are appropriate. The PAS logic also monitors plant status, and automatically reverts to manual operating mode when a major change in plant status occurs (for example, reactor scram or turbine trip).

(2) Semi-Automated Operation

The PAS also includes a semiautomatic operational mode that provides automatic operator guidance for accomplishing the desired normal changes in plant status. The operator must activate all necessary system and equipment controls for the semiautomatic sequence to proceed. The PAS monitors the plant status during the semiautomatic mode in order to check the progression of the semiautomatic sequence and to determine the appropriate operator guidance to be activated.

(3) Manual Operation

The manual mode of operation in the ESBWR corresponds to the manual operations of conventional BWR designs in which the operator determines and executes the appropriate plant control actions. The manual mode provides a default operating mode in the event of an abnormal condition in the plant or the failure of automation. The operator can completely stop an automated operation at any time by simply selecting the manual-operating mode.

3.3.5.4 *Staffing and Qualifications*

The HFE team develops a concept of operations indicating personnel staff composition and the roles and responsibilities of individual staff members based on anticipated staffing levels. The concept identifies the relationship between personnel and plant automation by specifying the responsibilities of the crew for monitoring, interacting, backing-up, and overriding automations and for interacting with computerized procedures systems and other computerized operator support systems.

3.3.5.5 *Mockups, Part-Task Simulation, and Full Scope Simulation*

Mockups, part-task simulations, and full-scope simulators provide for:

- Developing and validating the HSI
- Developing and validating requirements for procedures
- Training and qualifying operators
- Re-qualifying operators

Simulators range from those that emulate a portion of the plant or a system (part-task simulators) to those that fully reproduce the control room environment (full-scope simulators). Both have been used to facilitate HSI designs that support safe, efficient and reliable operator performance during all phases of normal plant operation, abnormal events and accident conditions, as well as for maintenance, test, surveillance, and inspection activities. To achieve operator performance goals, information, displays, controls, and other interface devices in the control room and other plant areas are systematically designed and implemented consistent with good HFE practices.

3.3.5.6 *Tests and Evaluations*

The HFE team develops testing and evaluation plans for the HSI designs that are iteratively conducted throughout the HSI development process. The types of tests and evaluations performed vary depending on the specific point in the design process.

The methodology used for testing applies the following criteria:

Trade-Off Evaluations

To adequately consider human performance the HFE team uses the following example factors when performing trade-off analyses and evaluations to make design choices.

- Personnel task requirements
- Human performance capabilities and limitations
- HSI system performance requirements
- Inspection and testing requirements
- Maintenance requirements
- Use of proven technology (Reference 2.1.1(3)) and the operating experience of predecessor designs

The HFE team makes trade-off evaluations to determine the relative benefits of selected design alternatives.

Performance-Based Tests

The HFE team plans performance-based tests to address the specific questions and design features being addressed. The tests and selection of participants, depends on the purpose of the evaluation, the questions being addressed, and the maturity of the design. The performance measures consider measurement characteristics, identification and selection of variables, and performance criteria. Test bed selection is based on test requirements and design maturity.

To the degree possible the test design minimizes bias, confounds, and error variance (noise). Design solutions are developed to address problems that are identified during the testing and evaluation of the HSI design.

The following performance measures are included in the test plan, as appropriate, for the specific test being performed:

- System measures relevant to plant safety (avoiding alarm conditions and technical specification violations)
- Personnel primary task performance (task times and procedure violations)
- Personnel errors (intention errors related to assessing the plant conditions, and execution errors related to using the HSI)
- Situation awareness
- Workload (cognitive: decision making; physical: motion)
- Personnel communications and coordination (information sharing and coordinated control actions, and crew synchronization)
- Dynamic anthropometry evaluations (reach and dexterity issues)
- Physical positioning and interaction with the HSI (physical motion between panels and workstations and information display-space navigation)
- Secondary task control (display format navigation, information search, etc.)

HSI Design Analyses, Reviews and Evaluations

This section provides a description of the methods and tools to be used for analyses, reviews and evaluations of the HSI during the design process.

Techniques appropriate for the evaluation of HSI include, but are not limited to:

- Checklists
- Structured interviews
- Direct observation of operator behaviors
- Analysis of historical records of operational problems with similar equipment
- Physical measurements
- Experiments
- Subject Matter Expert (SME) rating of alternative designs

The following are criteria that may be used in selecting HFE techniques:

- Safety and/or risk significance
- Type of design (taking into account the type of design, there are some techniques that may not apply)
- Type of technology.
- Relative time to perform
- Relative complexity
- Relative cost
- Relative cost effectiveness
- Demonstrated by use of dynamic displays, simulator, etc.

The design evaluation is based on the objectives of the systems design. What should the system do, who will use it, where will it be used and when will it be used? If the objectives are clear, the evaluation of the results is made simpler. Numerous methods are available for evaluation of designs.

Definition of the Design/Evaluation Tools for the HSI Design Analyses

Checklists, drawings, mock-ups, questionnaires, and interviews will be used, as described below, to gather HSI Tests and Evaluations data and information.

Design Criteria Checklist

A checklist includes a series of equipment and facility design requirements, taken from human engineering standards and guides, that address HSIs. The checklist is divided into categories of design criteria corresponding to major equipment or facilities. These categories might consist of visual displays, audio, controls, etc. NUREG-0700 provides examples of checklist formats.

Drawings

Engineering drawings or sketches of interest to the HFE Design Team may be further categorized as:

- Hardware drawings
- Workspace layout drawings
- Console drawings
- Panel arrangement drawings

Mock-ups

Mock-ups are constructed and used as tools in the development of the HSI to evaluate the system design before the actual manufacture of system hardware.

Mockups will provide a basis for resolving access, workspace and related human engineering problems, and incorporating these solutions into HSI design.

Functional mockups may be provided in those design areas where systems/equipment involve critical human performance and where human performance measurements are necessary.

In addition to the performance of normal, abnormal, and emergency evaluations, the mock-up is also used to evaluate maintenance, test, and inspection activities. Based on the fidelity of the mock-up, volume studies may be performed to assess equipment pull-space, personnel, and tool envelopes.

Questionnaires and Interviews

Questionnaires and interviews are used for obtaining information about the problems and positive system features that have been noted in the course of evaluations.

(1) Questionnaires

The questionnaire is a subjective measurement tool for systematically obtaining attitudinal responses from a selected group of individuals. The questionnaire provides a structured method for asking a series of questions in order to obtain measurable expressions of attitudes, preferences, and opinions. The questionnaire is used to assess a wide variety of qualitative variables such as acceptance, ease of use and preference.

(2) Interviews

The interview technique is the process of the evaluator discussing the test events with the participants.

The purpose of an interview is to find out either objective facts related to the system about which the interviewee has some knowledge, or subjective information, attitudes, or opinions about how the interviewee feels about some test aspect.

Test and Evaluation Methods for Evaluating and Resolving HFE/HSI Design Issues

The Evaluation Process

Evaluation is an integral part of the design process, with the results of evaluation efforts leading to interaction through the other phases of the design process. Therefore, planning for evaluation proceeds in parallel with design rather than after a prototype design has emerged.

It is necessary to establish the objectives of the design prior to the evaluation.

The evaluation process, which is to be efficient in terms of both time and cost, is an integral part of design. The evaluation process is iterative in the sense of including multiple phases of evaluation, with the results of each phase being used to enhance the design of the system as necessary to meet HFE goals.

The combined objectives of efficiency and design-oriented successive refinement dictate that the overall evaluation process includes multiple evaluation methods. Alternative methods may range from checklists or paper/electronic evaluations to part-task and full-scope simulator evaluations. The sequencing of these methods depends on the nature of the evaluative issues being addressed. There are three basic types of issues:

(1) Compatibility

A system is compatible to the extent that the physical presentations to the operator and the responses expected from the operator are consistent with human input-output abilities and limitations.

(2) Understandability

A system is understandable if the structure, format and content of the operator-system dialogue result in meaningful communication.

(3) Effectiveness

A system is effective to the extent that it supports an operator (or crew) in a manner that leads to improved performance, results in a difficult task being less difficult, or enables accomplishing a task that could not otherwise be accomplished.

Methods of Evaluation

Electronic, paper and part-task simulator evaluation methods are used in the design phase. Full-scope simulator and in-plant evaluation methods are used in the integrated verification and validation process.

(1) Electronic Evaluation

The primary purpose of the electronic evaluation is to assess compatibility in the sense of determining the degree to which a design takes advantage of MCR operator's abilities while avoiding their limitations.

Since much of the documentation and design is being developed on computers, an electronic version of documentation is available early in the design phase allowing for evaluating and resolving HFE/HSI design issues.

(2) Paper Evaluation

The results of a typical paper evaluation include a list of problems identified (human engineering deficiencies) and recommendations for modifying the system to eliminate the problems.

In order to expand the scope of a paper evaluation to include understandability and perhaps a few effectiveness considerations, the design team carefully analyzes the system design to see that it satisfies information requirements and to assess, if possible, the degree to which system objectives are achieved.

The paper evaluations of compatibility are performed, using HFE guidance.

It should be noted that both the electronic and paper evaluation methods are used in either a static or "dynamic" evaluation process. When used statically, the images (either on paper or electronic screen) are examined from a human factors perspective. When used dynamically, the images are used in a talk-through process to verbalize what is expected to appear in a specified event, and to examine this from a human factors perspective.

(3) Simulator Evaluation

A wide range of part-task simulators is possible, with static mockups on the low end.

The primary objective of part-task simulator evaluation is to assess understandability. As discussed earlier, this involves determining whether operators can comprehend the messages transmitted to them by the system, and whether they can communicate their desires, and perhaps intentions, to the system.

The purpose of evaluating understandability is to assess the validity of the answers generated during design by answering the following questions:

a. Do operators actually comprehend the messages presented by the system?

b. Do operators correctly formulate responses to these messages?

c. Do operators correctly communicate their responses to the system?

Dynamic simulation techniques are used as a human engineering design tool when necessary for the detail design of equipment requiring critical human performance. Consideration is given to use of various models for the human operator, as well as man-in-the-loop simulation. The simulation equipment is intended for use as a design tool, although its use as training equipment is considered in any plan for dynamic simulation.

3.3.5.7 *Procedures*

Human factor improvements in plant procedures help prevent or mitigate potential human error. Procedure development supports improvements in the HSI, plant hardware (e.g. in ergonomic layout), training, and other areas. The approach to reducing human error is to simplify the information reaching the operating personnel and to enable control room personnel to have a clear understanding of the plant status at any time. Through the HSI and procedures, operating personnel control the plant under normal, abnormal, and emergency conditions. As shown in Figure 1, the ESBWR is designed using a systematic process for integrating human factor engineering principles into the system design as well as the procedures that are used to operate the plant. Figure 1 also demonstrates how the HFE procedure development plan is an integral part of the MMIS and HSI development for the ESBWR.

Procedures specific to the ESBWR design and operating philosophy are developed or modified to reflect the characteristics and functions of the ESBWR plant improvements. As the details of the HSI are finalized, the V&V processes shown in Figure 1 support evaluation of the HSI and the procedures. To verify complete integration and consistency in the procedures, human factors principles are applied to both the hardware and procedure development aspects of the HSI. Tools, such as dynamic simulators that represent the control room HSI, the plant response to selected events, and the operator control actions taken, are used to validate the integrated design.

Information flow analysis is conducted for each of the categories of CBPs including normal, abnormal, and emergency procedures including EOPs and SAMGs.

3.3.5.8 *Panels and Consoles*

Main Control Console

The workstation for licensed reactor operators that operate the controls in the MCR is the main control console. It is configured such that each operator is provided with controls and monitoring information necessary to perform assigned tasks and allows the MCR operators to view all of the displays on a WDP from a seated position.

The design of the information and controls located at the operator workstation is integrated with the design of the mimics displayed on the WDP for consistency in nomenclature, symbols, and color.

The HSI design includes features, which facilitate operator activities that tend to keep the operators alert and attentive. Features of the HSI are designed based upon applicable industry research and publications to assure operator vigilance. The basis for the features, including a review of the experience of selected HSI features, is part of the documented design.

The main control console, in concert with the WDP, provides the controls and displays required to operate the plant during normal plant operations, abnormal events and emergencies. The main control console controls and displays include the following:

(1) The grouped workstations, controls, displays, and equipment used by control room personnel to monitor and control ESBWR operation

(2) Nonsafety-related on-screen control VDUs for non-safety system control and monitoring, and safety system monitoring, driven by the N-DCIS

(3) Safety-related on-screen control VDUs for safety system control and monitoring, driven by the Q-DCIS. The operation of these VDUs is fully independent of the N-DCIS

(4) Fixed-position, dedicated function switches, controls, or other equipment specified in the operational analysis requirements processed in HSI design

3.3.5.9 *Control System*

The control system is the combination of software constructs and hardware interfaces used by operators to interact with the HSI and plant equipment. Each of the controls is selected, presented, and set up to operate based upon options presented in the style guide that best meet the operational analysis requirements for the control. Additionally, the aggregate control presentation for a system or display screen is designed in accordance with the style guide. This process ensures that the combination of computer and hardwired controls used to operate the ESBWR individually and collectively meet HFE requirements and goals including:

- Control displays are consistent and easy to read including:
  - Size coding
  - Shape coding
  - Color coding
  - Status coding (open, closed, on, off)
  - Control variable displays (temperature, flow, pressure)
  - Control versus display only coding
  - Overall display structure
  - Display hierarchy for multi-screen control displays
  - Links to trending, monitoring, assistance automation, procedure, or other HSI control assistance features
- Control point labeling is consistent with end device designation and name
- Input devices are appropriate for the application considering required accuracy, duration active input is required, and work space limitations including options such as (adapted from NUREG-0700):
  - Cursor keys
  - Touch screens
  - Light pens
  - Mouse
  - Trackball
  - Joystick
  - Hardwired controls (rotary, rocker, toggle, thumbwheel, etc.)
- Controls that are easy to identify
- Control operation is in manner and direction in keeping with convention
- Controls that react and provide feedback in keeping with convention
- The existence of feedback indicating to the worker how effective his/her decisions and control actions were

3.3.5.10 *Display System*

VDUs Driven by the N-DCIS

A set of on-screen control VDUs is incorporated within the main control console for the following functions and tasks:

(1) Monitoring of plant systems, both safety and nonsafety-related

(2) Control of nonsafety-related system components

(3) Presentation of system and equipment alarm information

The N-DCIS displays and controls nonsafety-related systems including the alarm system. The N-DCIS is independent from the safety-related safety systems and their associated processors. All systems, safety and non-safety may be displayed on the nonsafety-related VDUs, but safety-related systems may only be controlled from the safety-related system VDUs.

VDUs Driven by the Q-DCIS

Safety-related VDUs that are physically separate, and functionally independent, of the N-DCIS are installed within the main control console. The VDUs are dedicated, divisionally separated devices, and qualified with supporting display-processing equipment, to safety-related standards. These VDUs are only used for monitoring and control of equipment within a given safety division.

3.3.5.11 *Alarms*

Alarm presentation provides for the display of certain key alarms or similar alarm-like information, which needs to be brought to operator attention. The specific items to be displayed as alarms are determined in the HSI design process for the alarm system. Additional alarms are presented within the display screen of the HSI and prompt the attention of operators where appropriate. Alarm functions are designed using the physical characteristics and functional characteristics set forth in the style guide.

Alarms are presented in a manner and intensity in keeping with their significance and risk. Alarm presentation possibilities include single parameter, grouped, combined, trip point, trend, or calculational variables that have alarming requirements specified in operational analysis. Alarms integrated into the HSI and displayed on VDUs may be displayed with linked controls, trends, indications or procedures.

Following the occurrence of an event or transient, actuation of the appropriate alarms:

- Alert operators to off normal conditions, which require them to take action
- Redirect the operators, to the extent possible, to the appropriate response
- Assist the operators in determining and maintaining an awareness of the state of the plant and its systems or functions
- Minimize distractions and unnecessary workload placed on the operators by the alarm systems

3.3.5.12 *Workstations*

Workstation Configuration

The physical elements of the HSI are organized into workstations at which plant personnel carry out the tasks of monitoring and controlling the ESBWR. Workstations can be stand-up, sit-down or a combination of both. HFE principles governing attributes such as reach, field of vision, and comfort are integral to the options contained in the HSI style guide and are therefore incorporated into the design.

Size and shape of HSI equipment such as: control consoles, desks, boards, panels and chairs are determined from the anthropometric requirements and other human engineering considerations. Details considered during workstation design include (adapted from NUREG-0700):

- Workstation height (operators, supervisors, and any other)
- Benchboard slope, angle, depth, available lay down space
- Control device locations
- Display device locations
- Accommodations for human body positioning including leg clearances, arm rests, etc.

Display and control equipment layout

Style guide HFE principles address both individual elements of the HSI and their grouping. The aggregate main control console, RSS stations, and LCS workstation configurations are consistently and logically laid out to enhance human awareness, understanding, control, and long-term use. Details considered during workstation layout design include (adapted from NUREG-0700):

- Grouping of related controls
- Placement of controls to provide ease of access and minimize inadvertent actuation
- Placement and arrangement of display devices
- Overall grouping of controls and displays

3.3.5.13 *Workplace*

(1) Space

The operator work area has sufficient space to allow performance of all necessary actions. Attention is paid to providing work areas, writing space, and storage space for documents:

a. Work areas manned on a continuous basis are designed for seated operation and adequate seating is provided. The workstations do allow for standing operations as well.

b. Where writing and access to documentation are normal parts of HSI duties, adequate writing space is made available. Laydown space for documents in use is available.

c. Storage space for documents is provided close to the operating position to avoid the documents being laid on consoles, desks, etc.

(2) Configuration

The HSI is designed giving due consideration to:

a. ESBWR operating principles

b. Allocation of Functions

c. Standardized ESBWR design determines the extent of controls present in the control room

d. Supervision criteria, which determine the number of VDUs and the extent to which hardwired controls are required, if any

e. ESBWR fleet-wide owners group technological options and preferences (choices)

f. The control room has operating areas where each operator obtains access to all controls and information required to perform the assigned tasks under operational and accident conditions

g. The operating area and HSI equipment such as control desks, boards, and panels are arranged according to HFE principles

Grouping of operating areas

The MCR and LCS are divided into operating areas where each operator has all the controls and indications required to perform the tasks assigned in various operating conditions including start up, normal operation, shutdown and emergencies. Consideration is also given to tasks related to maintenance, testing, and inspection activities. The configuration minimizes interference among operator tasks.

Control Boards and Arrangement

The arrangement of control panels, desks and boards in the MCR, RSS stations, and LCSs include:

a. Allowing each operator to have sufficient space among the panels for immediate and direct access to the information and controls pertinent to tasks

b. Eliminating conflicting paths for the various operators

c. Facilitating communications and coordination among the operators

3.3.5.14 *Environment*

Environmental conditions in the MCR are such that the operators can perform tasks effectively and comfortably. The environmental conditions are consistent with the MCR habitability requirements.

The MCR environmental specification includes requirements for:

(1) Heating, Ventilation and Air-Conditioning

The MCR ventilation system design accommodates postulated accident conditions of the plant. The HSI is designed in accordance with the MCR environmental conditions.

(2) Illumination

MCR lighting system gives special attention to uniformity, and control of shadows, glare, reflections, and highlighting.

An emergency lighting system continuously provides illumination necessary for task performance even on failure of the normal system.

(3) Auditory Environment

Auditory environment of the HSI is designed considering a relevant database on human auditory capability and characteristics.

3.3.5.15 *Communications*

Communications capability options presented in the HSI style guide cover the full operating spectrum of the ESBWR including normal, abnormal, and emergency operations. Provisions are made for clear verbal communications in and near operator workstations. Additional provisions are made for communications with one or more persons at remote locations. Distance communication options presented in the style guide include:

- Sound powered phones
- Conventional telephones - attributes to be considered include:
  - Robustness and reliability of emergency communication links
  - Locations of access points
  - Characteristics of equipment chosen such as microphone and speaker clarity, sensitivity, robustness, frequency ranges, noise limiting enhancements, and volume controls
  - Ergonomic considerations including handset or remote ear piece shape, keypad and display readability, cord length or wireless range, etc.
  - Ability for selected stations to override and break into communications to ensure that emergency communications can take place
- Radio wave based devices such as personal digital assistants, cell phones, portable radios, pagers, and hand held computers. Attributes to be considered include:
  - Clarity
  - Coverage in required areas
  - Verifiable compatibility with plant equipment in usage areas (electromagnetic interference/radio frequency interface studies completed)
  - Robustness of equipment
  - Data handling, processing, input, storage, and transmission capabilities
  - Ergonomic considerations including handset or remote ear piece shape, keypad and display readability, wireless range, etc.
  - Need for and positioning of repeaters
- Public address systems attributes to be considered include:
  - Access and input mechanism (microphone, telephone handset, or other)
  - Receiving location(s) and the ability to choose specific announcement areas
  - System usage: normal, emergency, fire, evacuation, etc.
  - Locations that can access the system

- Ability to override communications of lesser significance
- Intercoms
- Computer based communications including e-mail, electronic logs, instant messaging, and formal record keeping. Computer based communication attributes to be considered include:
  - Ability to perform the necessary communication functions in parallel and without interference to plant control and monitoring activities
  - Ability to draft, edit, cancel and address messages at will prior to sending or saving
  - Permanent and retrievable archiving of all official plant communications
  - Ability to edit or annotate saved official plant communications meeting all applicable regulatory and QA program requirements for such changes
  - Automatic time and user stamping of messages
  - Ability to group or link communications, such as log entries to provide continuity when communication involves several messages extending over time

3.3.5.16 *Software*

In addition to providing the vehicle by which the other HSI attributes presented in this plan are displayed and provide user input/output capability, HSI software incorporates, or provides links to, supporting software based administrative programs such as:

- LCO tracking
- Clearance process
- Operator log keeping
- Corrective action program
- Work management program
- Risk evaluation/management program
- Electronic permanent records storage program

3.3.5.17 *Graphical User Interface*

Graphical user interface (GUI) is prepared and used as a design input to the N-DCIS for HSI. This helps to ensure consistency in VDU design with inputs from different team participants or suppliers. The GUI style guide applies to GUI displays used in the MCR for both VDUs and GUIs used at safety-related local panels in the plant.

3.3.5.18 *SPDS*

The principal purpose of the SPDS is to aid control room personnel during abnormal and emergency conditions in determining the safety status of the plant and in assessing whether abnormal conditions warrant corrective action by operators to prevent core damage. During emergencies, the SPDS serves as an aid in evaluating the current safety status of the plant, in executing symptom-based emergency operating procedures, and in monitoring the impact of engineered safeguards or mitigation activities.

The SPDS is required to be designed so that the displayed information is readily perceived and comprehended by the MCR staff. Compliance with this requirement is assured because of the incorporation of accepted HFE principles into the overall implementation process. All of the continuously displayed information necessary to satisfy the requirements for the SPDS are included in the fixed-position displays and the SPDS design is implemented using the guidance from NUREG-0737, Supplement 1, NUREG-1342 and NUREG-0700, Section 5 to confirm that all applicable criteria are met. Selection of the parameters for inclusion in the SPDS display is based, in part, upon the ESBWR emergency procedure guidelines (EPGs). The SPDS also operates during normal operation, continuously displaying information from which the plant safety status is readily and reliably assessed. Principal functions of the SPDS are integrated into the overall control room display capability in a manner which complies with of NUREG-0737, Supplement 1.

4. IMPLEMENTATION

4.1 CONCEPT DESIGN

Conceptual design and style guide development take place in parallel with each other and as new operational analysis elements become available. Operational analysis requirements dictate control, monitoring, interface capabilities, and attributes that must exist in the HSI design. As these requirements are processed within the HSI design process, conceptual design possibilities are developed and considered. The HFE design team performs the research and analysis required to create the style guide criteria for the HSI element being considered. This criterion is then applied to the element and similar elements in the future. The interaction between HSI conceptual design and style guide is an iterative process and takes place throughout the HSI conceptual design.

The conceptual design translates operational analysis requirements and HFE principles contained within style guide specifications into design specifications.

4.1.1 Assumptions

The three phases of the HSI design process (concept design, style guide, and detailed design) utilize the same basic assumptions listed below:

- ESBWRs are operated as a standardized fleet of nuclear plants
- The training program, procedures, and HSI designs are generic to the ESBWR
- All normal, abnormal, and emergency operating procedures use the same names and numbering of plant equipment and HSI controls, indications, and presentations used by the plant operators
- The ESBWR is designed to operate with many passive systems and the HSI design provides for the standby readiness monitoring of these systems and verification of their performance when called upon to operate
- The control systems for the ESBWR have a high level of automation. Systems are automated unless regulation or HFE analysis results dictate otherwise.
- Computer based functions used by operators in the MCR, RSS stations, or LCSs with a safety-related function or as defined by TA are imbedded in or accessed through the HSI
- CBPs are accessible anywhere the HSI can be accessed, with the exception of the Q-DCIS
- SPDS displays can be viewed anywhere the HSI is accessible

4.1.2 Inputs

Requirements Developed from Operations Analyses

Operations analyses (SFRA, AOF, and TA) results provide the basis for the design of the HSI.

The SFRA determines the performance requirements and design considerations of the HSI design and establishes the functions, which are accomplished to meet these requirements.

The allocation of functions to personnel, systems or personnel-system combinations is made to reflect: sensitivity, precision, time and safety requirements, required reliability of system performance, and the number and level of skills of personnel required to operate each system.

The TA identifies the behavioral requirements of the tasks associated with individual functions.

Types of requirements identified in the TA include:

a. Information and Decision-Making Requirements
b. Response Requirements
c. Feedback required for monitoring and evaluating the adequacy of actions taken
d. Cognitive and physical workload demands
e. Task Support Requirements
f. Workplace Factors
g. Staffing and Communication Requirements
h. Potential Hazard Identification
i. A minimum list of critical parameters for design

The HSI design is based on the staffing requirements defined in the S&Q plan. The MCR staff size and roles are finalized after the completion of the V&V activities.

Operating Experience Review of Previous NPP MMIS Designs

Operating experience lessons learned from events, operational problems, and enhancement opportunities from previous plant HSI designs is gathered, categorized, and provided to HSI designers. This information has been gathered and maintained in the OER/BRR database for generating lessons learned involving HFE issues. It is used to correct and enhance HSI design issues to improve overall HSI effectiveness. This process also provides for the continuous review and improvement of the HSI as ESBWR specific operating experience is gathered over time.

Both updated domestic and modern foreign nuclear power plants operating experience are reviewed as available. The operating experience information is used by engineers and designers to support the development of HSI design requirements and features that mitigate human error.

Other Industries

The HFE Design Team reviews HSIs being used in other industries such as fossil plants, aerospace, petrochemical, etc., for features and approaches applicable to the ESBWR. Some design features used in other industries and considered for use in the ESBWR HSI include:

- Use of flat panel and Video Display Unit (VDU) displays
- Use of electronic on-screen controls

- Use of a Wide Display Panel (WDP)
- Use of prioritized alarm systems
- Automation of process systems
- Operator workstation design integration

OERs are performed on potential applications and include:

- Review of reports provided by industry organizations (NRC, INPO, etc.)
- Review of applicable research in these design areas, as may be documented in reports from universities, national laboratories, the NRC, and in proceedings published by HFE professional societies
- Review of applicable research and experience reports published by HSI equipment vendors

The OER in each of the three areas specified above also includes feedback obtained from actual users. If the documents selected for the conduct of the OER for a particular area do not include the results of user feedback, then interviews with users of at least two applications of that particular technology area are also conducted.

4.1.3 Process

HFE criteria are applied, along with other design requirements, to select and design the particular equipment for application to the MCR and RSS stations HSI. The HSI design implements the information and control requirements that have been developed in the TA, including the displays, controls, and alarms necessary for the execution of those tasks identified in the TA as being critical tasks. The configuration of the equipment design is established to satisfy the functional and technical design requirements and the design process ensures the HSI is consistent with HFE principles.

The HSI design criteria applied to the ESBWR MCR is also used in the design of the information displayed on the VDUs located in the TSC and EOF. The information displayed in the TSC/EOF and Emergency Operating Procedures (EOPs), a subset of information, is available to the operator in the MCR. HSI, as defined for ESBWR, also includes the operator interface at the RSS stations displays and LCSs with a safety-related function or as defined by TA.

Typically, the order in which various kinds of HSI are addressed is dictated by the amount of lead-time required for construction, progressive availability of design information, and time needed to satisfy training requirements. Human factors efforts are completed within the overall plant development schedule. HSI development is performed in accordance with the MMIS and HFE Implementation Plan Reference 2.1.1(3).

Physical layout of the plant is determined early so that building construction can begin. MCR workspace interfaces are considered first. Panel design proceeds within constraints of workspace design decisions. Communications system interfaces are next considered, within constraints of workspace and panel design decisions.

Evaluation of at least some parts of communications system design is completed in sufficient time for equipment to be used in final stages of personnel training. The design of HSI is performed using the integrated systems approach.

Human factor design criteria have been developed through experience and evaluation of previous interface designs. Applicable human capabilities and characteristics for the project are provided as fundamental human factors design data, consistent with the top-down approach. Such data include HFE requirements that are directly applicable to the plant staff for the MCR, RSS stations, and other HSI. The data also includes HFE requirements that are applicable to operators and maintenance staff. Related areas include the following:

(1) Anthropometric considerations

(2) Population human perceptual system capabilities

(3) Auditory and visual capabilities and characteristics

(4) Human ability to process information

4.1.4 Outputs

The output of conceptual design defines the basic form, content, equipment, layout, and environment used by plant personnel to monitor and control the ESBWR during all phases of plant operation. Operational analysis requirements are incorporated in accordance with HSI style guide criteria to ensure the safe and efficient operation of the plant in normal, abnormal, and emergency conditions. Conceptual design provides for:

- Information display
- User-system interaction
- Process control and input devices
- Alarm systems
- Analysis and decision aids
- Inter-personnel communication
- Computer based procedures
- HSI software
- Workplace design

Significantly more detail regarding some of the specific attributes of these outputs is available in Section 4.3.

An additional output from the conceptual design process is design options and criteria for use in the development and refinement of the style guide. Information flow is a two way iterative process that continues throughout the design process.

4.2 HSI SPECIFIC GUIDANCE – STYLE GUIDE

Options for satisfying operational analysis requirements are selected and evaluated for use in the ESBWR HSI. Those that are approved by the HFE design team for possible use in the ESBWR HSI are incorporated into the style guide. Additionally, requirements, attributes, supporting details, presentation formatting and any other supporting detail that the HFE design team associates with the HSI element being considered is incorporated into the style guide. The HFE infused style guide design guidance created in this fashion ensures consistency of design between the MCR, RSS stations, and LCSs with a safety-related function or as defined by TA as well as between the sub elements of each of these control centers.

4.2.1 Assumptions

The three phases of the HSI design process (concept design, style guide, and detailed design) utilize the same basic assumptions listed below:

- ESBWRs are operated as a standardized fleet of nuclear plants
- The training program, procedures, and HSI designs are generic to the ESBWR
- All normal, abnormal, and emergency operating procedures use the same names and numbering of plant equipment and HSI controls, indications, and presentations used by the plant operators
- The ESBWR is designed to operate with many passive systems and the HSI design provides for the standby readiness monitoring of these systems and verification of their performance when called upon to operate
- The control systems for the ESBWR have a high level of automation. All systems are automated unless regulation or HFE analysis results dictate otherwise.
- All computer based functions used by operators in the MCR, RSS stations, or LCSs with a safety-related function or as defined by TA are imbedded in or accessed through the HSI
- CBPs are accessible anywhere the HSI can be accessed
- SPDS displays can be viewed anywhere the HSI is accessible

4.2.2 Inputs

The requirements generated in operational analysis are inputs to the conceptual design phase where various options for hardware and software are considered. Each of these options is input to the style guide element analysis where it either becomes an HSI design element option with associated HFE usage and supporting detail specifications, or is rejected as an option for use in the ESBWR. The technical option inputs are analyzed using HFE principles and practices provided by the HSI design team HFE specialist, along with the desired attributes established in the operations analysis. Options selected are used to generate style guide HSI element alternatives with associated human factors usage specifications.

The training, procedures, V&V, and HPM processes provide feedback inputs that can result in revisions to the lists of allowable elements and their specifications and requirements contained in the style guide.

4.2.3 Process

The style guide is created using input from similar guides from previous designs such as the ABWR, HSI style guides from other industries, NUREG-0700, and other applicable documents. As operational analysis requirements are processed for implementation in the HSI design, the HSI design team will consider existing alternatives contained in the style guide. If style guide alternatives do not adequately address the requirement being considered or if potential enhancements to options are proposed, then additional HSI element options are evaluated for use in the ESBWR HSI. If approved, the new element options are incorporated into the style guide and are made available for use by HSI design team. The style guide is a compilation of HSI equipment, control, display, interface, and structures from which designers can select the most appropriate alternative for a given application. Additionally, the style guide sets requirements for when and how to incorporate the various hardware alternatives.

Similar guidance is provided in the area of HSI software including workstation design and presentation content, format, and logic. Style guide requirements maintain consistency in presentation, navigation, and interface mechanisms between various portions of the HSI.

This iterative process continues throughout the HSI design process.

4.2.4 Outputs

The output of the style guide design activity is a document presenting hardware, software, and usage alternatives from which the HFE design team constructs the ESBWR HSI. Additionally, the guide outlines the basic requirements and formatting specifications associated with each alternative incorporated into the HSI. The guide is a living document that takes input from the conceptual design process (HSI design elements being considered). The guide in turn provides input back into the conceptual design process in the form of approved human factors alternatives and usage specifications. Through this iterative process, the HSI design team is provided the flexibility and the HFE guidance to create an HSI that meets ESBWR goals.

The ESBWR style guide information is specific to the project and typically is more detailed than that contained in HFE guidance documents such as NUREG-0700. Appendix A provides the work process that develops the ESBWR style guide. Figure A-1 provides examples of the type of information that is contained in the ESBWR style guide.

4.3 HSI DETAILED DESIGN

The detailed design uses the alternatives and features selected in the conceptual design process and the guidance contained in the style guide to generate detailed HSI designs. The detailed design process addresses hardware, software, layout, formatting, and features incorporated into the HSI design to meet ESBWR human centered design goals.

4.3.1 Assumptions

The three phases of the HSI design process (concept design, style guide, and detailed design) utilize the same basic assumptions listed below:

- ESBWRs are operated as a standardized fleet of nuclear plants
- The training program, procedures, and HSI designs are generic to the ESBWR
- All normal, abnormal, and emergency operating procedures use the same names and numbering of plant equipment and HSI controls, indications, and presentations used by the plant operators
- The ESBWR is designed to operate with many passive systems and the HSI design provides for the standby readiness monitoring of these systems and verification of their performance when called upon to operate
- The control systems for the ESBWR have a high level of automation. All systems are automated unless regulation or HFE analysis results dictate otherwise.
- Computer based functions used by operators in the MCR, RSS stations, or LCSs with a safety-related function or as defined by TA are imbedded in or accessed through the HSI
- CBPs are accessible anywhere the HSI can be accessed
- SPDS displays can be viewed anywhere the HSI is accessible

4.3.2 Inputs

The basic design of the ESBWR HSI is created during the conceptual design. The established design elements are input to the detailed design process where required supporting design features and characteristics are identified. They include:

- HSI requirements and design characteristics developed from operating experience and literature analyses, tradeoff studies, engineering evaluations and experiments, and benchmark evaluations, as well as records of the basis of the design changes
- Detailed HSI descriptions including its form, function, and performance characteristics
- The results of tests and evaluations performed in support of HSI design

4.3.3 Process

Human factors specialists work closely with other development team participants and confer with the project architect-engineers to identify design constraints for the size and shape of control room. They help to coordinate control system engineering concerns with layout alternatives, suggesting advantageous console configurations and profiles and recommending arrangements of major furnishings. Human factors specialists also interact with lighting system engineers, heating and air-conditioning engineers, decorators, and other design specialists responsible for decisions that influence environmental conditions and other aspects of control room habitability. They also assess preliminary layouts, identifying potential performance degrading effects of design features and recommending ways to overcome them. The project human factors specialists are given sign-off authority for drawings at each step in control room design to ensure that human factors issues are adequately addressed.

The design team assesses the interactive implications of proposed main control console profiles and configurations with respect to the control room size and shape. The main control console profiles and dimensions must be consistent with the defined user population, regulatory guidance (for example, NUREG-0700) and the utility requirements. General requirements for ambient environmental conditions in the control room are defined as well as recommendations for preliminary layout of the MCR.

The steps included are the following:

(1) Define proposed MCR dimensions

The MCR is as compact as possible while accommodating all necessary equipment and allowing for freedom of movement in performing assigned tasks. A compact MCR reduces walking and viewing distances associated with task performance, enhances unaided voice communications, and discourages incursions by unauthorized visitors. The size and shape are established as follows:

a. Identify architectural-engineering constraints

b. List major equipment that must be accommodated

c. Estimate dimensions of required floor space

(2) Define proposed main control console configurations

The main control room panel system description presents the MCR operator panels and the large display panel design based on the ESBWR DCD and the inputs from the standard plant design process. To define proposed MCR configurations:

a. Consider advantages and disadvantages of different types of configuration using results of operational analysis

b. Select proposed MCR configurations

(3) Define proposed main control console profiles

a. Determine appropriateness of standing, seated, or sit-stand console profiles

b. Adjust profile for operator viewing

c. Determine relation to console profiles in other plant locations

d. Select proposed main control console profiles

(4) Assess interactive implications of proposed main control console selections

(5) Define general requirements for ambient environmental conditions

Human engineering principles and criteria are applied to design of work environments. Drawings, specifications and other documentation for work environment, MCR staff, facilities, and MMIS reflect incorporation of human engineering requirements under normal, abnormal and emergency conditions.

After proposed main control console configurations and profiles have been defined, and their iterative implications for MCR size and shape have been assessed, the ambient environmental conditions necessary to support personnel performance are generally defined as follows:

a. Determine lighting requirements

b. Identify ways to moderate sound

c. Consider influences of surface properties in the control room

d. Specify climatic conditions

(6) Produce recommendations for MCR preliminary layouts

a. Consider the criteria included in the applicable regulatory guidelines, and utility requirements in preparing MCR preliminary layout recommendations

b. Locate operator furnishing in relation to consoles

c. Provide access space, for example, for repair and testing activities

d. Ensure adequate storage space for MCR staff and safety equipment

e. Locate provisions for shift supervisor's activities

f. Establish means for limiting visitor access

g. Locate personal conveniences, for example, restroom, locker, kitchen

h. Locate aisle way doors for personnel passage

(7) Review of alternative designs by HFE team

(8) Define dimensions for selected main control console profiles

(9) Define detailed design features for desks and other furnishings

(10) Identify hazard avoidance features

(11) Define specific lighting features

4.3.4 Outputs

4.3.4.1 *Control Room Interfaces*

Visible and Audible Coding

Coding principles are established in an early stage of HSI design. The coding principles are consistent with guidelines of NUREG-0700. The coding system is consistent throughout the HSI. This applies to location, information, color, and illumination codes. Coding is consistent among HSI in the MCR, LCS, and back panels.

Simulator coding is consistent with the plant MCR. The equipment symbols, abbreviations, and acronyms are defined in the DCD. Use of symbols for coding of components should be consistent with the shapes defined in the DCD. New shapes are defined and documented in the style guide.

The coding method selected for application is determined considering the relative advantages of the types of coding.

Coding method and guidelines are as follows:

(1) Physical Coding.

a. Size coding - Not more than three different sizes are used for discrimination by absolute size

b. Shape coding - Number of shapes is limited in shape coding

c. Color-coding - The number of colors used for coding is kept to the minimum to provide necessary information. Less than eight colors are preferable and not more than 12 colors, including black and white, are used.

To ensure the correct use of color-coding, the following rules are applied:

i. Color is used in a redundant mode. This is necessary to allow for variations in lighting conditions.

ii. The choice of colors allows all users to discriminate between each color under all conditions of use.

iii. The colors used contrast adequately with the background of the display. In addition, adjacent colors contrast adequately with each other.

iv. Consistency of meaning assigned to each color is essential. The use of color codes with symbols is consistent across all applications within the control room and LCS.

v. For VDU display, the background color is pure and free from noise patterning.

vi. In selecting color codes, common human perception of the color meaning (for example, red-alarm, yellow-caution, etc.) as well as industry standards and practices which have been identified for advanced control rooms are used.

d. Auditory coding - Auditory coding by frequency is permissible but not more than five separate frequencies should be used. Auditory coding may be implemented based on frequency, rate of change, patterns, and location of auditory device.

e. Intensity coding - Use of intensity coding should be minimized (that is, contrast between two characters on a screen) on visual displays.

(2) Information Coding.

Coding of displays can improve the usability of the information by aiding comprehension and assimilation. The code employed enhances the flow of information from the process to the user and does not require the user to decipher information in order to use it.

The most important factor of the code is to enhance discrimination.

Purely abstract codes such as arbitrary associations of items with data are avoided because they are difficult to learn and use.

(3) Location Coding (structuring coding).

The use of consistent relative positioning of information reinforces the intended message in addition to the information transmitted by a pointer, character, a group of characters or a symbol.

(4) Data Coding.

A major use of data coding is abbreviations. Abbreviations used on labels, displays and VDU formats comply with a standardized set of abbreviations based on formal rules, which meet the user population needs. Abbreviations are used consistently between VDUs, labels, etc. Coding on VDU displayed information is consistent with coding used on the WDP. This includes the use of colors and abbreviations.

Abbreviations and acronyms for the ESBWR project are defined in the DCD. New abbreviations or acronyms are identified and documented in the place of use (that is, document, drawing, etc.).

(5) Enhancement coding.

Enhancement coding is used to reinforce the data being transmitted. The available techniques include reverse video and blinking of 3 Hz to 5 Hz on VDU displays and symbol size and style brightness on all types of displays.

Labeling

Adequate labeling is provided in the control room. The labeling is consistent with NUREG-0700, other labeling in the plant, and in accordance with accepted HFE practices and principles for readability by the user population. Additional guidelines related to labeling are found in applicable documents in the style guide.

Labeling criteria includes:

(1) System and components are labeled and labels are readily visible by plant personnel

(2) Labels are designed and mounted so that text is oriented horizontally for ease of reading

(3) The format of presentation (for example, order, position) is consistent on all labels

(4) The acronyms and abbreviations utilized are easily identifiable to the full names, concise, and consistently used throughout the systems, SDSs, drawings, and procedures

(5) Characters used on labels are sized for optimum viewing with considerations for the local environment conditions (for example, illumination)

4.3.4.2 *Human Centered Design*

ESBWR HFE design team has modified an operator decision-making model that identifies four major cognitive activities supported by the HSI:

- Detection and monitoring/situation awareness
- Interpretation and planning
- Control

- Feedback

Detailed HSI design supports human centered design goals by providing support for both rule based and knowledge based modes of operation. HSI computer based procedures and their supporting assistance features coupled with support for any paper based procedures used by operators, ensures rule based operational goals are met. HSI resources are also designed to promote knowledge-based operations. HSI system data, alarm condition, and parameter trending presentation capabilities support knowledge-based operations including event diagnosis, and decision-making.

4.3.4.3 *Automation Design*

The AOF portion of operational analysis determines where responsibility for performance of plant monitoring and control tasks is assigned. Those functions and tasks allocated to machine or shared performance (machine-human limited, machine-human backup, human-machine limited, or human machine backup) have automations designed to support performance of the operational analysis requirements. Software management plans referenced in Reference 2.1.1(3), ESBWR Man-Machine Interface System and Human Factors Engineering Implementation Plan, lay out how the software supporting the required automations is designed, developed, tested and implemented. The following is a very brief description of each automation class (Reference 2.1.2(2)):

Machine Only – the function is executed entirely by plant automation. Humans have no direct control, backup, or limiting actions associated with the function(s) being allocated.

Machine, Human Limited – This output allocates the function to plant equipment and automation for performance. This performance is limited in one or more steps in the function data structure sequence by required human action of some kind. The required action can be an acknowledgement of a HSI queue alerting the operator to impending action or it can be more detailed. One example of when this allocation is selected is where economic impacts may result if the machine sequence continues.

Machine, Human Backup – This output allocates the function to plant equipment and automation for performance. Plant personnel monitor the machine and perform or complete performance of the function in the event that the machine does not complete its execution. Analysis has shown that while the machine is best suited to perform the function sequence, plant personnel are capable of performing the sequence if called upon. Additionally, analysis has determined that the consequences of partial or incorrect performance are such that operator performance of the functions following machine failure is warranted.

Human, Machine Assist – This output allocates the function to plant personnel for performance. Equipment and automation assist plant personnel in performance of the function. Analysis has shown that the human is capable of mitigating the consequences he may make. One or more forms of machine assistance are provided to aid in the performance of the function.

Human, Machine Backup – This output allocates the function to plant personnel for performance. The machine monitors human performance of the function and performs or completes performance of the function in the event that the human does not complete its execution. Analysis has shown that while the human is best suited to perform the function sequence, potential error consequences are unacceptable and the machine is capable of mitigating the consequences of potential human errors.

4.3.4.4 *Staffing and Qualifications*

The HSI design process receives input from the S&Q process when establishing HSI conceptual design specifications. Conceptual design combines the requirements and ownership allocations generated in operational analysis with the most appropriate human owner based upon qualifications and number of personnel available in the required location.

Feedback is provided from HSI detailed design to the staffing and qualification and operational analysis processes when the design process is unable to generate detailed design output that meets the requirements concurrently. Additionally, feedback is provided in the form of cumulative workload for specific staff positions and qualifications for use in workload analyses.

4.3.4.5 *Mockups, Part-Task Simulation, and Full Scope Simulation*

The detailed HSI design is used to develop mockups, part task simulators, and full scope simulators that emulate the final plant design. These mockups and simulators are used to V&V the work performed and the results obtained during implementation of the HFE design process shown in Figure 1.

Training for all normal, abnormal, and emergency operating conditions is validated through simulator testing where applicable, or through mockups. NUREG-0711 sets forth test objectives and testbed validation guidelines that are discussed in the V&V plan. As shown in Figure 1, the V&V process supports HFE evaluation of the HSI design, normal, abnormal, and emergency operating procedures and their CBP equivalents, and the output of the training plan.

In addition to testing stand-alone procedures, a test process is developed to verify that the separate procedures convert into an integrated set of procedures. These procedures have a common language and the names of systems and components are consistent throughout the procedure set. The test process includes dynamic simulation of startup, power operation, and shutdown. During power operation the alarm response procedures and abnormal operating procedures are simulated to verify that trained operators respond properly. V&V is performed using a variety of means including part-task simulations, talk through evaluations, walk through evaluations using mock-ups, and full scope simulation.

The process includes dynamic simulation of startup, power operation, and shutdown. Any issues identified during the V&V process are provided as feedback to the originating process for resolution. Based upon the nature of the issue, procedures may be revised, HSI design may be modified, or the issue is input to the training program so that operators are taught the conditions necessary for consideration during plant operations. The priority for modifying the HSI design, procedures, or training in response to a human factor discrepancy is guided by an assessment of risk impact from the PRA/HRA interface.

4.3.4.6 *Tests and Evaluations*

Appropriate design tools and techniques are selected to analyze the HSI design, depending on the nature of the aspect being evaluated. There are two main types of HSI analysis. The first analysis verifies that the HSI design meets established human factors criteria. The second analysis verifies that the HSI meets other technical requirements established as design requirements from TA, operator evaluation, and applicable plant procedures.

(1) Techniques that are appropriate for the evaluation of HSI include, but are not limited to:

  a. Checklists
  b. Structured interviews
  c. Direct observation of operator behavior
  d. Analysis of historical records of operational problems with similar equipment
  e. Physical measurement
  f. Experiments
  g. SME rating of alternative designs

(2) Criteria that may be used in selecting HFE techniques are the following:

  a. Safety and/or risk significance
  b. Type of design (taking into account the type of design, there are some techniques that may not apply)
  c. Type of technology
  d. Relative time to perform
  e. Relative complexity
  f. Relative cost
  g. Relative cost effectiveness
  h. Demonstrated by use of dynamic displays, simulator, etc.

The design evaluation is based on the objectives of the systems design. What should the system do, who will use it, where will it be used and when will it be used? Numerous methods are available for evaluation of designs. See Appendix B for more detailed test and evaluation work process.

4.3.4.7 *Procedures*

An implicit design goal in most discussions of human-system interfaces is that system design enables users, to be in control of the technology.

Procedures enable users to accomplish daily tasks adequately. However, without at least a common-sense understanding of how the procedures relate to the underlying system, users are unable to adapt them to new situations, to deal with either system malfunctions or the consequences of their own errors, or to adapt to new or evolving systems.

The HSI pertinent to procedures and their use is applied in meaningful ways that accommodate these concerns. A basis of user system understanding is developed along with procedures. Thus full generalization and well-informed procedure development and use are enabled.

4.3.4.8 *Panels and Consoles*

The physical elements of the HSI are organized into workstations at which plant personnel carry out the tasks of monitoring and controlling the ESBWR. Workstations are stand-up, sit-down or a combination of both. HFE principles governing attributes such as reach, field of vision, and comfort are integral to the alternatives contained in the HSI style guide and are therefore incorporated into the design.

Size and shape of HSI equipment such as: control consoles, desks, boards, panels and chairs are determined from the anthropometric requirements and other human engineering considerations. Details considered during workstation design include (adapted from NUREG-0700):

- Workstation height (operators, supervisors, and any other)
- Benchboard slope, angle, depth, available lay down space
- Control device locations
- Display device locations
- Accommodations for human body positioning including leg clearances, arm rests, etc.

Display and control equipment layout

Style guide HFE principles address both individual elements of the HSI and their grouping. The aggregate main control console, RSS stations, and LCS workstation configurations are consistently and logically laid out to enhance human awareness, understanding, control, and long-term use. Details considered during workstation layout design include (adapted from NUREG-0700):

- Grouping of related controls
- Placement of controls to provide ease of access and minimize inadvertent actuation
- Placement and arrangement of display devices
- Overall grouping of controls and displays

The primary design function served in this portion of the detailed HSI design is the aggregate HFE treatment of the workstations and displays at a given control location.

4.3.4.9 *Control Systems*

Control Display Integration

Controls and their associated displays are integrated to ensure effective operation of the plant. Control-display integration is in accordance with the proposed method of plant operation as identified in the operations analysis performed for each system by the HFE Design Team.

The control-display integration meets the following principal requirements:

(1) Hardware controls should be located near the associated display. Operation of controls should produce a compatible change in the relevant display

(2) The operation of systems and components by "soft" and "hard" switches. (Soft switches are controls located in the VDUs)

(3) The selection of the type of control is consistent with operator needs to navigate or take process control action, and with the associated guidance provided in NUREG-0700

(4) The grouping of controls and their associated displays reflect the need to achieve system objectives that are consistent with the user's mental thought process

(5) Where sequence of use is a key factor, the organization of controls and displays reflects cause/effect relationships

(6) The organization of controls takes into consideration any user population stereotype groupings

The form of codes used for displays and their associated controls is consistent between the MCR and RSS.

4.3.4.10 *Display Systems*

The HSI display system is designed with consideration for the human capabilities and characteristics of the user population.

(1) The major functional requirements of the display system are as follows:

   a. The display system covers appropriate variables, consistent with the assumptions of the safety analysis and with the information needs of the operator in normal operation and accident conditions. The accuracy and range of displays are consistent with the assumptions of the safety analysis.

   b. A display is provided for showing bypassed or deliberately inoperable conditions of plant and auxiliary systems

   c. Safety-related information displays are suitably located and specifically identified

   d. Appropriate types of displays are developed depending on the intended purpose for the displayed information

   e. The display system also considers support for maintenance, test, and inspection activities

(2) There are many types of displays available such as:

   a. Display with Indicators and Lamps

   Information display arrangements with analog or digital indicators, indication lamp, illuminated graphic symbols, etc., are made based on human characteristics and ergonomic considerations.

   Principles of the location aids such as coding by color, shape, etc., are applied to those indicators, lamps, etc., themselves. Scales of analog indicators and the movement of indication are consistent to changes of relevant process variables and the population human perceptual system capabilities.

b. VDU Displays

The major functional requirements for VDU displays are as follows:

i. Necessary information is available to the operator whenever it is required

ii. The display communicates the intended information to the operators without ambiguity or loss of meaning

iii. Symbols are standardized and the range of symbol sizes is limited

Direction of process flow paths and sequence events in schematic displays should be in accordance with population human perceptual system capabilities and mimics on control room panels.

VDU displays are designed considering human factors and design criteria shown above and should be compatible with both the associated controls and instrumentation and the perceptual and cognitive needs of an operator.

c. Large Screen Displays

Consider using large screen displays when:

i. A group of operators is required to interact as a team based on the same information

ii. One or more operators are required to move about, and require frequent referral to information to make decisions

iii. Space or other considerations such as a limited number of individual displays preclude the use of individual displays for each team member to call up the commonly used information

It may be desirable to have general (for example, overview or summary) information available to persons who should not interrupt ongoing group operations by looking over the shoulders of individual operators to view their individual displays.

Direct-view or projection VDU systems offer the advantage of allowing use of displays developed for smaller screens. If screen size is limited by space or other considerations, existing displays may be redesigned using larger characters and symbols to achieve the character heights required.

d. Large Wall-Sized Fixed Mimic

The HSI design includes an integrating overview mimic in the MCR. This mimic meets the requirements for integration into the HSI design process.

This mimic is intended to support the operation team approach to control activities by providing a spatially dedicated, continuously available reference to the status of equipment defined by TA.

The overview mimic provides for the display of a limited number of critical plant operating parameters. The specific parameters are determined in the design process, to enable the operators to shutdown the reactor.

The overview mimic provides for the display of the system equipment operational status, for example, flow or no-flow, energized or de-energized, on or off, open or close, etc., of a limited number of components defined by TA. The specific displays are determined in the design process; however, the following are considered for incorporation:

i. Reactor vessel

ii. Feedwater and condensate system pumps

iii. Containment Isolation valves

iv. Safety systems valves

v. RWCU/SDC pumps and valves

vi. Power supply breakers

vii. Auxiliary power supply breakers

viii. Safety and relief valves

ix. Circulating water pumps

e. Design of Displays

The requirements of a display or suite of displays are determined with a proper and systematic analysis of the proposed use of the data being displayed. For each proposed item of information, the HSI designer should consider the following attributes:

i. For whom is the data required? Formats should be structured or revised to meet operator needs.

ii. For what purpose or purposes is the data required? (For example, maintenance data are separated from operational data)

iii. Whether comparisons with other data on VDU formats or other displays are required

iv. When is the data required? (For example, relevance to operator actions)

v. The accuracy with which the data are read

vi. The characteristics of the data in terms of rate of change, noise, etc.

vii. What errors of interpretation are acceptable, if any

viii. The degree of detail or abstraction, which is required

Following the occurrence of an event or transient only the following should appear as alarms:

i. Alert operators to off normal conditions, which require them to take action

ii. Redirect the operators, to the extent possible, to the appropriate response

iii. Assist the operators in determining and maintaining an awareness of the state of the plant and its systems or functions

iv. Minimize distractions and unnecessary workload placed on the operators by the alarm systems

The location of data display facilities should take into account the intended operational staffing levels, the assignment of operational responsibilities and functions and the need to optimize the number of displays consistent with adequate manning of each operator workstation. The latter consideration is dependent on anthropometric factors such as viewing angle, viewing distance, proximity to associated controls and indications, etc., and amount of data to be displayed.

The HSI design team identifies and documents bases and assumptions.

f. General requirements of VDU design

Displays should be as simple, clear and comprehensible as possible. Where complex or highly detailed displays are necessary, a good organization and structure are required.

The HFE design team uses a HSI design specification to assure that all applicable HFE practices and principles are applied in a consistent manner for all VDU display designs. The specification assures that the "look and feel" of all of the Graphical User Interfaces (GUI) is consistent. The specification is based on a GUI style guide applicable to the HSI.

Where safety criteria require raw, unprocessed data to be presented in addition to the processed information, the display organization and identification differentiate between the two types of information. The HSI design is consistent with the design specifications and the applicable references for HFE guidelines.

i. Availability

Necessary information is displayed to the operator whenever it is required.

ii. Legibility

Information shown on VDU is clearly presented in all operating conditions.

To obtain the necessary legibility of the VDU, the format specification is based on HSI documents and design team recommendations.

iii. Accuracy

The display communicates the intended information to the operator without ambiguity or loss of meaning. The scaling of graphs and histograms enables the operator to resolve indications adequately and the maximum or current value is annotated with the numerical value on the graph. For digital displays, the number of decimal places displayed matches the required accuracy of the measurements.

iv. Consistency

Standardization of displays can be beneficial, but it does not take precedence over the more important criteria defined above.

All items within a suite of displays, which represent the same information, should be similarly named.

When using the same items on different displays they should be consistent for each display. This includes data fields, symbols, etc. Grouping techniques should be consistently applied with standardized headings and style.

g. Form of presentation, use of symbols and graphics

The most important design principle is to make the display as simple and clear as possible, while not losing either essential detail or important principles and relationships.

i. The display format needs to consider operator issues in dealing with high rates of information changes during transient and trip conditions

ii. Suitable logic for prioritizing the information flow is needed to minimize the potential for information overload

iii. The time resolution for displays should address realistic operator needs, considering transients in the ESBWR inherently occur slower than in previous BWR plants

Symbols are standardized and the range of symbol sizes is limited to a progression, which allows easy recognition of the various sizes.

Related plant items are organized in a way that reflects their functional relationship with the appropriate degree of abstraction being employed, yet avoid complicating the display. The presentation should be compatible with other related forms of information display within the same location. Use of grouping and coding techniques for enhancement of the perceptions of displayed information is important.

Process flow paths and event sequence should generally progress from left-to-right and from top-to-bottom, in accordance with population human perceptual system capabilities. Schematic displays on the VDUs should be formatted and oriented in accordance with the fixed-position mimic.

Sequence and message construction should present good syntax and where possible a standardized hierarchical message structure should be employed.

The layout of information should reflect the sequence, if any, in which it is used. Rows of tabular information are normally divided into groups of not more than five.

4.3.4.11 *Alarms*

(1) Alarm System Purpose

An alarm system is the basic operator support system for managing abnormal situations and has the following two functions:

a. The primary function of the alarm system is to warn the operator about a situation that is not normal. The warning function helps the operator control the future behavior of a complex plant by drawing attention to undesired process conditions.

b. The secondary function of the alarm system is to serve as an alarm and event log. The log function supports the operator's need to analyze the events that have lead to the current or previous process conditions.

In addition to the alarm system, a number of other information sources may be important in the management of abnormal situations, such as trending, video surveillance, overview displays, process simulations and advanced condition monitoring.

(2) Design and Operation

a. The alarm system design is based on an alarm philosophy, which constitutes the basic rationale for the alarm system

b. Every alarm requires an operator response, either physically or mentally. If the event does not require such a response, it is an event, not an alarm

c. Design to ensure that the alarm system remains usable in all process conditions, by ensuring that unacceptable demands are not placed on operators thereby exceeding their perceptual and cognitive capabilities. The aim is to configure the alarm limits in such a way that the operators have time to carry out an action before an automatic shutdown action is taken.

i. Maximize use of combined and computed alarms

ii. Use combined and computed alarms for suppression of alarms with less information content

iii. Alarm message content should minimize the need for information recall from long-term memory

d. Alarm limits are based on:

i. Plant mode, status, and situation dynamics

ii. Shutdown, Tech Spec, and component limits

iii. Likely rate of change of the signal during off-normal conditions

iv. Response time of the operator to correct the condition

Moreover, for each alarm, a procedure document, (for example, alarm sheet or alarm response procedures) are provided to explain to the operator the likely reasons of the alarm and the corrective actions required. Computer based operator aids may be used for explaining the importance of particular combinations of alarm signals.

(3) Display of Alarms

The display of alarms on alarm-tiles, the WDP or on VDUs meets the following:

a. Combining relevant process and alarm information in the WDP mimic display provides spatially dedicated alarm overview under all process conditions, improving management of alarm overload

b. Alarms are integrated into process displays, using symbols and icons close to the components or functions to which they are related

c. An alarm is presented as a visual and audible cue in close proximity to where the operator can take corrective action.

d. Any new alarm starts an audible warning and flashes a tile light or VDU symbol

e. An alarm may be steadied after it has been acknowledged

f. The steadied alarm is indicated to ensure that its existence is not forgotten

g. When the cause of alarm has been corrected, the alarm display may be returned to the normal mode manually or automatically. In either case, the control room staff is notified by audible and visual cues that the cause has been corrected.

h. Navigation in alarm displays allows quick access to additional information, such as online alarm procedures, and to displays that offer more, real-time detail

Alarm Processing Logic

Alarm prioritizing and filtering logic enhances the presentation of meaningful alarm information to the operator and reduces the amount of information the operators must absorb and process during abnormal events.

Signal filtering is used to prevent measurements that fluctuate around their alarm limits from generating useless, repeated alarms that are a nuisance and might contribute to alarm flooding. Low pass filtering and dead-bands can remove process noise and fluctuations around the alarm limit. Dead-bands may be adjustable by the operator with administrative controls. Time-delay and time limit mechanisms may also be employed where low pass filtering is not possible.

Alarm suppression, on the other hand, is used to ensure that the presented alarms at any time are relevant to the operator's most important task under the current plant conditions and to avoid alarm flooding. Alarm suppression must be documented in such a way that it is familiar and understandable to the operator. In order to trust the alarm system, it is important that operators understand why some alarms are suppressed while others are not.

Alarm suppression is based upon the following concepts:

- Suppression Based on the Operating Mode: The plant operating mode is defined on the basis of the hardware or process status, and alarms which are not relevant to the current operating mode are suppressed. For example, alarms, which are needed in the "RUN" mode but are unnecessary in the "SHUTDOWN" mode are suppressed.
- Suppression of Subsidiary Alarms: Alarms are suppressed if they are logically consequent to the state of operation of the hardware or to the process status. For example, scram initiation (a plant-level alarm condition announced with a fixed-position alarm tile on the WDP) logically leads to scram accumulator low pressure

(also an alarm condition). Such subsidiary alarms are suppressed if they simply signify logical consequences of the system operation.

- Suppression of Redundant Alarms: When there are overlapping alarms, such as "high" and "high-high" or "low" and "low-low", only the more severe of the conditions is alarmed and the others are suppressed.
- Suppress alarms for components that are out of order or unavailable due to maintenance, testing, etc.
- Even alarms that are suppressed under current conditions are available in detailed or special displays

4.3.4.12 *Workstations*

People come in different size and shapes. One workstation dimension that is suitable for one individual may be totally inappropriate for another. The goal, therefore, is to design workstations that fit the greatest number of people while inconveniencing the fewest.

Anthropometry relates to the physical dimensions of the work envelope, with two essential applications: to establish proposed workstation dimensions and, to evaluate existing workstations. The theory is to design workstations using anthropometric data so that workstations fit people, rather than forcing people to adjust to workstations.

By definition, anthropometrics is "the measurement, collection and use of data pertaining to such physical characteristics as shapes and size of human beings." A large portion of a given population is selected and measurements of body size and shapes are compiled in databases.

The goal is accomplished by fixing a dimension at a point where the majority of people "fit" or by making the workstation to allow for individual variances. For example, it is impossible to design an overhead clearance that is adjustable; therefore, doorways are designed to accommodate all but the most extreme statures. On the other hand, chairs are constructed easily with adjustable features to allow for individual variances.

Anthropometric data takes two forms: static data and dynamic data. Static data is derived from a person in static postures; dynamic data is based on movements, which approximate most work environments.

Regardless of the type of data, it follows a statistical phenomenon known as normal frequency distribution. When the frequency of occurrences is plotted on a graph against the actual measurement, it forms a normal (bell) frequency distribution curve. The significance of this is that designers of products, tools, equipment, etc., have a quantifiable design basis on which to make design decisions where human factors are involved.

At various points along the distribution curve, it is determined what percentage of the population fall below and above the given dimension. These points are referred to as percentiles. At the 50th percentile, 50 percent of the population is smaller or larger than the given size measurement. Likewise, at the 5th percentile, five percent are smaller and 96 percent are larger, and at the 95th percentile, only five percent are larger.

Using this information, it can be seen that there are definite dangers in using the 50th percentile in design criteria, as only half of the population would be accommodated unless adjustability was built in. In keeping with the desire to accommodate as many people as possible (and practical), normal design is for either the 5th or 95th percentile depending on the component in question.

4.3.4.13 *Workplace*

The proposed dimensions for the MCR and the consoles are defined to assure that the MCR arrangement allows for the necessary support staff work areas. The arrangement may be modified in accordance with the detailed human factors analysis and requirements.

4.3.4.14 *Environment*

Environmental considerations are taken into account to ensure that they do not adversely impact the ability of humans to effectively use the HSI. Environmental variables considered include:

- Noise
- Lighting
- Flooring and slip, trip, and fall potential
- Accessibility
- Vibration
- Temperature

4.3.4.15 *Communications*

Communication systems are provided to facilitate safe and efficient plant operation. Consideration is given to the design of communication systems to be used in the abnormal or accident conditions to communicate with the emergency facilities.

Access to the communication system should be administratively controlled.

Provision of nonverbal communication systems such as data-links (between computers), and other forms of message systems are desirable, between the control room, and other emergency facilities in order to provide secondary (backup) communications.

The communication systems are designed in accordance with accepted HFE principles, practices and guidelines as defined in the applicable documents.

Verbal Communication Systems

(1) On-site Telephone Communications

For general communication under normal operating conditions, a telephone system with a necessary number of extensions is installed. The telephone system allows the operations staff to preprogram telephone numbers. The number of extensions provided in the control room is based on the MCR operational requirements. The MCR telephone systems are designed in accordance with regulatory requirements for emergency response facilities. Capability is provided for communication among operators and maintenance technicians using portable, wireless communication equipment supported by appropriate base stations, antennas, amplifiers and/or repeaters. The voice communication systems are designed in accordance with operating utility requirements.

Voice communications systems and equipment are provided to support all phases of operations and maintenance, including emergency operations.

(2) Plant-wide Paging and In-plant Telephone System

A page system is provided to give capability of plant-wide paging of personnel.

Communication by radio to the control room using mobile transmitters is provided.

Operating radio frequency interference analysis is considered in the design, cabling, location and testing of the Instrumentation and Controls systems. Areas where transmitters may not be used, such as the control equipment room, are identified and appropriate warning signs posted.

(3) Off-site Communications

A speech and/or computer-based system are provided for communication to the off-site authorities and emergency, governmental and public agencies. These systems are designed to meet site-specific needs while complying with applicable regulatory requirements.

(4) Local Arrangement

The MCR is also designed as the communication center of the plant for normal operation and during the early stages of an accident. Communications equipment for communicating with locations off-site should be located on a special communication desk or panel with extensions on the MCR desk and other locations as appropriate.

Non-verbal Communication System

Non-verbal communication systems between the control room and emergency facilities are available in accordance with utility administrative controls for distribution of plant information. Data communication links between computers in the MCR and emergency facilities are in accordance with utility administrative controls.

4.3.4.16 *Software*

The system has data acquisition, display, and alarm functions. The system also has recording and memory functions for the plant process variables for analysis and for reporting within the operating organization and external authorities.

Information processing functions are provided to support high-level mental processing by the operator as a means of:

- Aiding decision-making
- Improving monitoring performance and capability
- Improving availability and reliability of information
- Providing feedback for organization of actions
- Improving communication among staff

- Improving a record of transients and accidents for analysis purposes

The information system provides data acquisition, data processing, display, and alarm functions for operators and non-shift support staff. The system also provides recording and printing functions.

The functions defined below are provided in the ESBWR through the HSI in the MCR. Plant status is also available at remote terminals located in the TSC, RSS stations, EOF, and LCS.

(1) Information for operators

In accordance with the design features of the ESBWR, the overall plant status is monitored by MCR operators using information presented on the wide display panel (WDP).

The operator is able to obtain, at any time, detailed plant information from the information presented in HSI VDUs

Visual and audio devices indicate deviations from normal operation. When these occur, the information systems enable the operators to:

a. Recognize any current or potential plant safety or availability hazards

b. Know the actions being taken by automatic systems

c. Analyze the cause of the disturbance and follow its course

d. Determine any necessary manual counteractions

The design basis for information systems, including their measurement devices, takes into account their risk importance. The intended safety function of each system and its importance in enabling the operators to take proper pertinent actions in anticipated operational occurrences or accident conditions are identified in the SFRA and are used as an input to any MMIS categorization method selected.

(2) Information function for non-shift support staff

Although the MCR is the information and control center of the plant for the operators during both normal operation and accident conditions, it may also be used as the primary center to direct the initial stages of off-site activities depending on national, state, local and utility principles for emergency operations support.

Information systems are extended to supply information to separate outside support facilities.

(3) Printing

An adequate number of printers are provided in or adjacent to the MCR to allow for hard copy output of process variables and chronological information about the performance and behavior of the plant.

Hard copy output of plant variables may be necessary for the following purposes:

a. Backup information for shift operators providing short-term and long-term trends

b. General operational information for plant management

c. Short-term and long-term analysis of operation, transients and accidents

Distributed Control and Information System (DCIS)

The requirements related to data acquisition and processing systems are covered in the ESBWR DCD Chapter 7, Instrumentation and Control Systems. The DCIS provides redundant and distributed control and instrumentation data communications networks to support the monitoring and control of interfacing plant systems.

These systems include electrical devices and circuitry (such as multiplexing units, bus controllers, formatters and data buses) that connect sensors, display devices, controllers, and actuators, which are part of these plant systems. The DCIS also includes the associated data acquisition and communication software required to support its function of plant-wide data and control distribution.

4.3.4.17 *Graphical User Interface*

Implementation User-Interface Design

The following points are guidelines to good software interface design. These guidelines apply to the content of screens. In addition to following guidelines, effective software also necessitates using techniques, such as 'storyboarding', to ensure that the flow of information from screen to screen is logical, follows user expectations, and follows task requirements.

(1) Consistency

a. Certain aspects of an interface should behave in consistent ways at all times for all screens

b. Terminology should be consistent between screens

c. Icons should be consistent between screens

d. Colors should be consistent between screens of similar function

(2) Simplicity

a. Break complex tasks into simpler tasks

b. Break long sequences into separate steps

c. Keep tasks easy by using icons, words, etc.

d. Use icons/objects that are familiar to the user

(3) Human Memory Limitations

a. Organize information into a small number of "chunks"

b. Try to create short linear sequences of tasks

c. Do not flash important information onto the screen for brief time periods

d. Organize data fields to match user expectations, or to organize user input (for example, auto-formatting phone numbers)

e. Provide cues/navigation aids for the user to know where they are in the software or at what stage they are in an operation

f. Provide reminders, or warnings as appropriate

g. Provide ongoing feedback on what is and/or just has happened

h. Let users recognize rather than recall information

i. Minimize working memory loads by limiting the length of sequences and quantity of information

(4) Cognitive Directness

a. Minimize mental transformations of information (for example, using 'control+shift+esc+8' to indent a paragraph)

b. Use meaningful icons/letters

c. Use appropriate visual cues, such as direction arrows

d. Use "real-world" metaphors whenever possible (for example, desktop metaphor, folder metaphor, trash can metaphor, etc.)

(5) Feedback

a. Provide informative feedback at the appropriate points

b. Provide appropriate articulatory feedback - feedback that confirms the physical operation you just did (for example, typed 'help' and 'help' appear on the screen). This includes all forms of feedback, such as auditory feedback (for example, system beeps, mouse clicks, key clicks, etc.).

c. Provide appropriate semantic feedback - feedback that confirms the intention of an action (for example, highlighting an item being chosen from a list)

d. Provide appropriate status indicators to show the user the progress with a lengthy operation (for example, the copy bar when copying files, an hour glass icon when a process is being executed, etc.)

(6) System messages

a. Provide user-centered wording in messages (for example, "there was a problem in copying the file to your disk" rather than "execution error 159")

b. Avoid ambiguous messages (for example, hit 'any' key to continue - there is no 'any' key and there's no need to hit a key, reword to say 'press the return key to continue)

c. Avoid using threatening or alarming messages (for example, fatal error, run aborted, kill job, catastrophic error)

d. Use specific, constructive words in error messages (for example, avoid general messages such as 'invalid entry' and use specifics such as 'please enter your name')

e. Make the system 'take the blame' for errors (for example, "illegal command" versus "unrecognized command")

(7) Anthropomorphization

a. Do not anthropomorphize (that is, do not attribute human characteristics to objects) - avoid the "Have a nice day" messages from your computer

(8) Modality

a. Use modes cautiously - a mode is an interface state where what the user does has different actions than in other states (for example, changing the shape of the cursor can indicate whether the user is in an editing mode or a browsing mode)

b. Minimize preemptive modes, especially irreversible preemptive modes - a preemptive mode is one where the user must complete one task before proceeding to the next. In a preemptive mode other software functions are inaccessible (for example, file save dialog boxes).

c. Make user actions easily reversible - use 'undo' commands, but use these sparingly

d. Allow escape routes from operations

(9) Attention

a. Use attention grabbing techniques cautiously (for example, avoid overusing 'blinks' on web pages, flashing messages, 'you have mail', bold colors, etc.)

b. Do not use more than four different font sizes per screen

c. Use serif or sans serif fonts appropriately as the visual task situation demands

d. Don't use all uppercase letters - use an uppercase/lowercase mix

e. Don't overuse audio or video

f. Use colors appropriately and make use of expectations

g. Do not use more than four different colors on a screen

h. Do not use blue for text (hard to read), blue is a good background color

i. Do not put red text on a blue background

j. Use high contrast color combinations

k. Use colors consistently

l. Use only two levels of intensity on a single screen

m. Use underlining, bold, inverse video or other markers sparingly

n. On text screens do not use more than three fonts on a single screen

(10) Display issues

a. Maintain display inertia - make sure the screen changes little from one screen to the next within a functional task situation

b. Organize screen complexity

c. Eliminate unnecessary information

d. Use concise, unambiguous wording for instructions and messages

e. Use easy to recognize icons

f. Use a balanced screen layout – do not put too much information at the top of the screen - try to balance information in each screen quadrant

g. Use plenty of 'white space' around text blocks - use at least 50% white space for text screens

h. Group information logically

i. Structure the information rather than just presenting a narrative format (comprehension can be 40% faster for a structured format)

(11) Individual differences

a. Accommodate individual differences in user experience (from the novice to the computer literate)

b. Accommodate user preferences by allowing some degree of customization of screen layout, appearance, icons, etc.

c. Allow alternative forms for commands (for example, key combinations through menu selections)

In order to effectively apply these design principles, one needs to understand users' tasks and requirements. Understanding and applying principles is meaningless if users are unhappy with the final product.

The goal for user interface design is to have the interface positively support users' endeavors and never intrude adversely. The interface should be transparent to the task the user is trying to accomplish and be efficient, satisfying.

Design Principles

Simplicity: Do not compromise usability for function

Keep the interface simple and straightforward. Users benefit from function that is easily accessible and usable. A poorly organized interface cluttered with many advanced functions distracts users from accomplishing their everyday tasks. A well-organized interface that supports the user's tasks fades into the background and allows the user to work efficiently.

Basic functions should be immediately apparent, while advanced functions may be less obvious to new users. Function should be included only if a TA shows it is needed. Therefore, keep the number of objects and actions to a minimum while still allowing users to accomplish their tasks.

Support: Place the user in control and provide proactive assistance

To give users control over the system, enable them to accomplish tasks using any sequence of steps that they would naturally use. Do not limit them by artificially restricting their choices to your notion of the "correct" sequence.

Most users perform a variety of tasks, being expert at some and novice at others. In addition to providing assistance when requested, the system recognizes and anticipates the user's goals, and offer assistance to make the task easier. Ideally, assistance provides users with knowledge that allows them to accomplish their tasks quickly.

Familiarity: Build on users' prior knowledge

Allow users to build on prior knowledge, especially knowledge they have gained from experience in the real world. A small amount of knowledge, used consistently throughout an interface, empowers the user to accomplish a large number of tasks. Concepts and techniques are learned once and then applied in a variety of situations. Users do not have to learn new things to perform familiar tasks.

The use of concepts and techniques that users already understand from their real world experiences allows them to get started quickly and make progress immediately.

In the past, designers tended to invoke a principle of consistency when no single design alternative appeared to be the best answer. By choosing to be consistent with something the user already understands, an interface can be made easier to learn, and more productive.

Avoid the tendency to employ consistency without understanding users, their tasks, and their shared experiences. When choosing a dimension within which to be consistent, seek to understand what the user expects and be consistent with those expectations. Providing a familiar experience is the ultimate use of consistency in which a truly intuitive interface results.

Obviousness: Make objects and their controls visible and intuitive

Where possible, use real-world representations in the interface. Real-world representations and natural interactions (direct action) give the interface a familiar look and feel and can make it more intuitive to learn and use. Icons and windows were early attempts to draw on user experiences outside the computing domain. As designs move toward real-world representations, reliance on such computer artifacts should decline. In an object-oriented interface the objects and concepts presented to users parallel familiar things from the real world; for example:

- Trash can - when things are thrown away, usually some type of trash receptacle or "trash can" is used. An object on the desktop displayed as a trash can communicates to users that it is a place for discarding things. It should look like the real object rather than like an abstract container, and the user should be able to show its contents in a meaningful way.
- Telephone - the actions taken with telephones are so familiar to most people that they require little thought. A telephone object on the desktop indicates to users that it allows them to perform phone-related tasks, and users expect it to behave like the real thing.

The controls of the system should be clearly visible and their functions identifiable. Visual representations provide cues and reminders that help users understand roles, remember relationships, and recognize what the computer is doing. For example, the numbered buttons on the telephone object indicate that they can be used to key in a telephone number.

Allow users to interact directly with objects and minimize the use of indirect techniques. Identifying an object and doing something with it (like picking up the handset of a phone to answer it) usually are not separate actions in the real world.

Encouragement: Make actions predictable and reversible

A user's actions cause the results the user expects. In order to meet those expectations, the HSI designer must understand the user's tasks, goals, and mental model. Use terms and images that match users' task experience, and that help users understand the objects and their roles and relationships in accomplishing tasks.

For applications other than plant control features, users should feel confident in exploring, knowing they can try an action, view the result, and undo the action if the result is unacceptable. Users feel more comfortable with interfaces in which their actions do not cause irreversible consequences.

Avoid bundling actions together, because the user may not anticipate the side effect. For example, if a user chooses to cancel a request to send a note, only the send request should be cancelled. Do not bundle another action, such as deletion of the note, with the cancel request. Rather than implementing composite actions, make actions independent and provide ways to allow users to combine them when they wish.

Satisfaction: Create a feeling of progress and achievement

Allow the user to make uninterrupted progress and enjoy a sense of accomplishment. Reflect the results of actions immediately; any delay intrudes on users' tasks and erodes confidence in the system. Immediate feedback allows users to assess whether the results were what they expected and to take alternative action immediately. The user can then decide if the effect is what was desired and, if not, can change it before switching attention to something else.

Offer a preview of the results of an action when it would be inconvenient for a user to apply the action and then reverse it. This saves the user a lot of time by not having to reverse the action that's been applied to an entire document and enhances the user's confidence in the system.

Avoid situations where users may be working with information that is not up-to-date. Information should be updated immediately or refreshed as soon as possible so that users are not making incorrect decisions or assumptions. This becomes especially important in networked environments where it is more difficult to maintain state between networked systems dynamically.

Availability: Make all objects available at all times

Users should be able to use all of their objects in any sequence and at any time. Avoid the use of modes, those states of the interface in which normally available actions are no longer available, or in which an action causes different results than it normally does.

Modes restrict the user's ability to interact with the system. Modal dialogs tend to lock users out of their system; to continue, users must complete - or cancel - the modal dialog. If users need to refer to something in an underlying window to complete the dialog, they must cancel the dialog, access the information they need and re-invoke the dialog.

Safety: Keep the user out of trouble

Users are protected from making errors. The burden of keeping the user out of trouble rests on the designer. The interface should provide visual cues, reminders, lists of choices, and other aids, either automatically or on request. Humans are much better at recognition than recall. Contextual and hover help, as well as agents, can provide supplemental assistance. Simply stated, eliminate the opportunity for user error and confusion.

Users should never have to rely on their own memory for something the system already knows, such as previous settings, file names, and other interface details. If the information is in the system in any form, the system should provide it.

Two-way communication may be necessary at times to allow users to clarify or confirm requests, or to remedy a problem. In the past, many interfaces have treated communication with users as primarily one-way, computer-to-user. The communication should be interactive - as rich in presentation and interaction capabilities as the rest of the interface. It presents relevant information, provides access to related information and help, and allows users to make task-specific decisions to continue.

Adopt the following design perspective: users know what they want to accomplish, but sometimes they find it difficult to express their desires using the objects and actions provided, and the system is unable to recognize their request. Two-way communication may be used to help users reach their goals.

Versatility: Support alternate interaction techniques

Allow users to choose the method of interaction that is most appropriate to their situation. Interfaces that are flexible in this way are able to accommodate a wide range of user skills, physical abilities, interactions, and usage environments.

Each interaction device is optimized for certain uses or users and may be more convenient in one situation than another. Pen input is helpful for people who sketch, and mouse input works well for precisely indicating a selection. Alternative output formats, such, as computer-generated voice output for foreign language instruction, are useful for some purposes. No single method is best for every situation.

Users are allowed to switch between methods to accomplish a single interaction. For example, allow the user to swipe-select using the mouse, then to adjust the selection using the keyboard. At the same time, users should not be required to alternate between input devices to accomplish what they perceive as a single step or a series of related steps in a task. Users should be able to complete an entire useful sequence through the same input device.

Providing a range of interaction techniques recognizes that users are individuals with different abilities and situations. The differences include disabilities, preferences, and work environments.

Affinity: Bring objects to life through good visual design

The goal of visual design in the user interface is to surface to the user in a cohesive manner all aspects of the design principles. Visual design should support the user model and communicate the function of that model without ambiguities. The final result should be an intuitive and familiar representation that is second nature to users.

The following are visual design principles that promote clarity and visual simplicity in the interface:

- **Subtractive design** - reduce clutter by eliminating any visual element that doesn't contribute directly to visual communication.

- **Visual hierarchy** - by understanding the importance of users' tasks, establish a hierarchy of these tasks visually. An important object can be given extra visual prominence. Relative position and contrast in color and size can be used.
- **Affordance** - when users can easily determine the action that should be taken with an object, that object displays good affordance. Objects with good affordance usually mimic real world objects.
- **Visual scheme** - design a visual scheme that maps to the user model and lets the user customize the interface. Do not eliminate extra space in your image just to save space. Use white space to provide visual "breathing room".

4.3.4.18 *SPDS*

Displays of critical plant variables, sufficient to provide information to plant operators about the following critical safety functions, are continuously displayed on the WDP as an integral part of the fixed-position displays:

- Reactivity control
- Reactor core cooling and heat removal from the primary system
- Reactor coolant system integrity
- Radioactivity control
- Containment conditions

Displays to assist the plant operator in execution of symptom-based emergency operating procedures are available at the main control console VDUs. Examples of these VDU displays are trend plots and operator guidance. Information regarding entry conditions to the symptomatic emergency procedures is provided through the fixed-position display of the critical plant parameters on the WDP. The critical plant parameters on the WDP are also viewable from the shift supervisors' console. The supplemental SPDS displays on the VDUs on the main control console are also accessible at the shift supervisors' console and are provided in the TSC and EOF. The SPDS displays are available to be viewed on display equipment defined by the utility.

Entry conditions to symptomatic emergency operating procedures are annunciated on the alarm windows on the WDP. The WDP also displays the containment isolation status, safety systems status, and other critical parameters.

5. RESULTS

5.1 RESULTS SUMMARY REPORT

The results of the HSI design process outlined in this plan are summarized in a Results Summary Report (RSR). The RSR provides a list of the design specifications for the HSI, instruments required to comply with regulations, and the HSI style guide developed during implementation of this plan. The RSR is written with sufficient detail to document how the methodology outlined in this plan was implemented to provide the results. In addition, the RSR outlines:

- General approach including the purpose and scope of HSI design
- HFE standards and documents used in the HSI design activity
- Concept of operations from an HSI perspective
- Functional requirement specification for HSIs
- Style guide and design specifications for HSI design including:
  - The development and basis for the guide
  - The scope and topical contents contained in the guide
  - Procedures used to maintain the style guide
- HSIs used in the MCR and RSS for the minimum inventory of alarms, displays, and controls presented in the DCD Table 18.1-1a and Table 18.1-1b, respectively
- List of instruments that complies with RG 1.97 and supporting analysis
- The methods used for the evaluation and verification of the HSI
- Overall assessment of how well the methodology and implementation of the procedure development process and results adhere to this plan

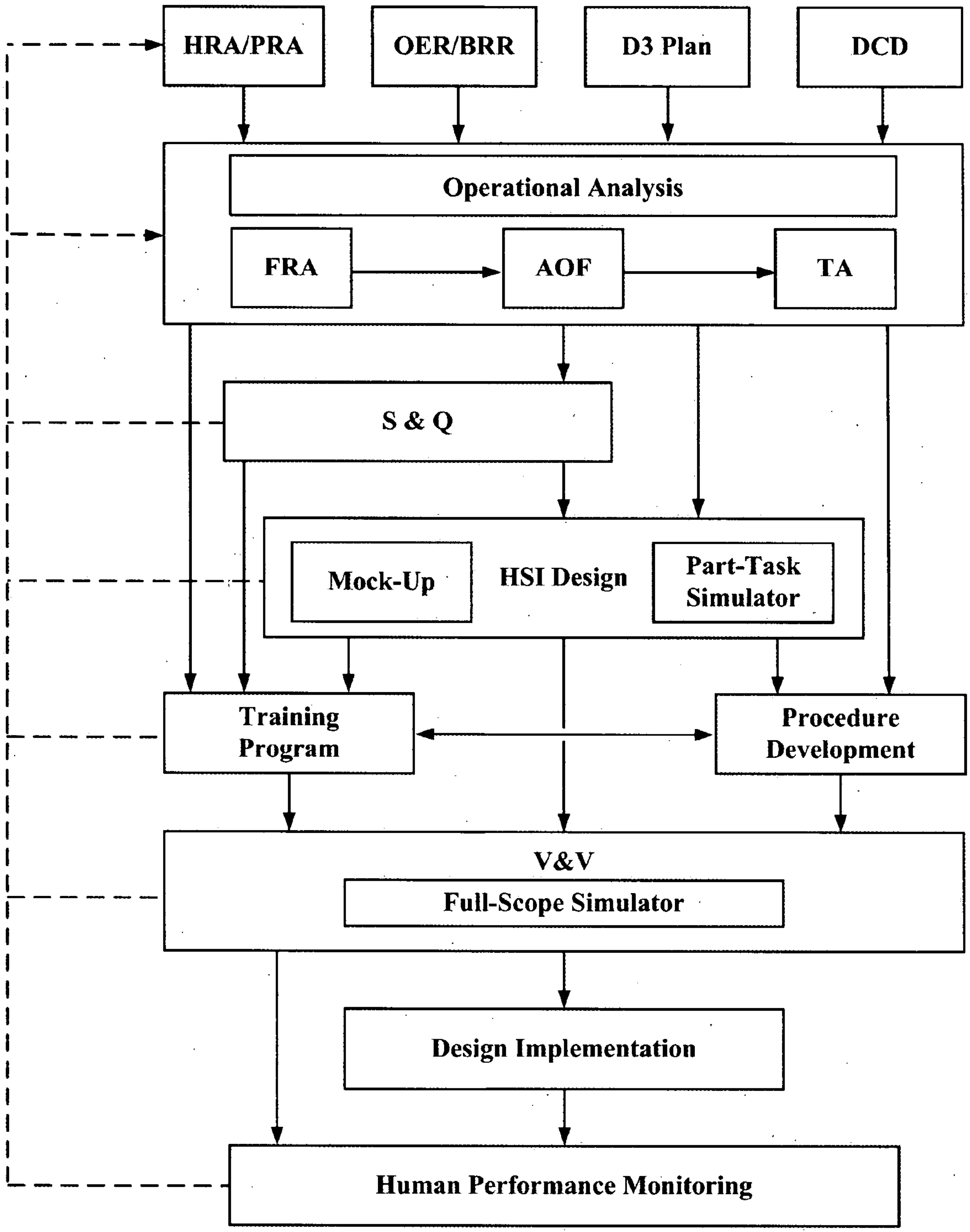

Figure 1. HFE Implementation Process

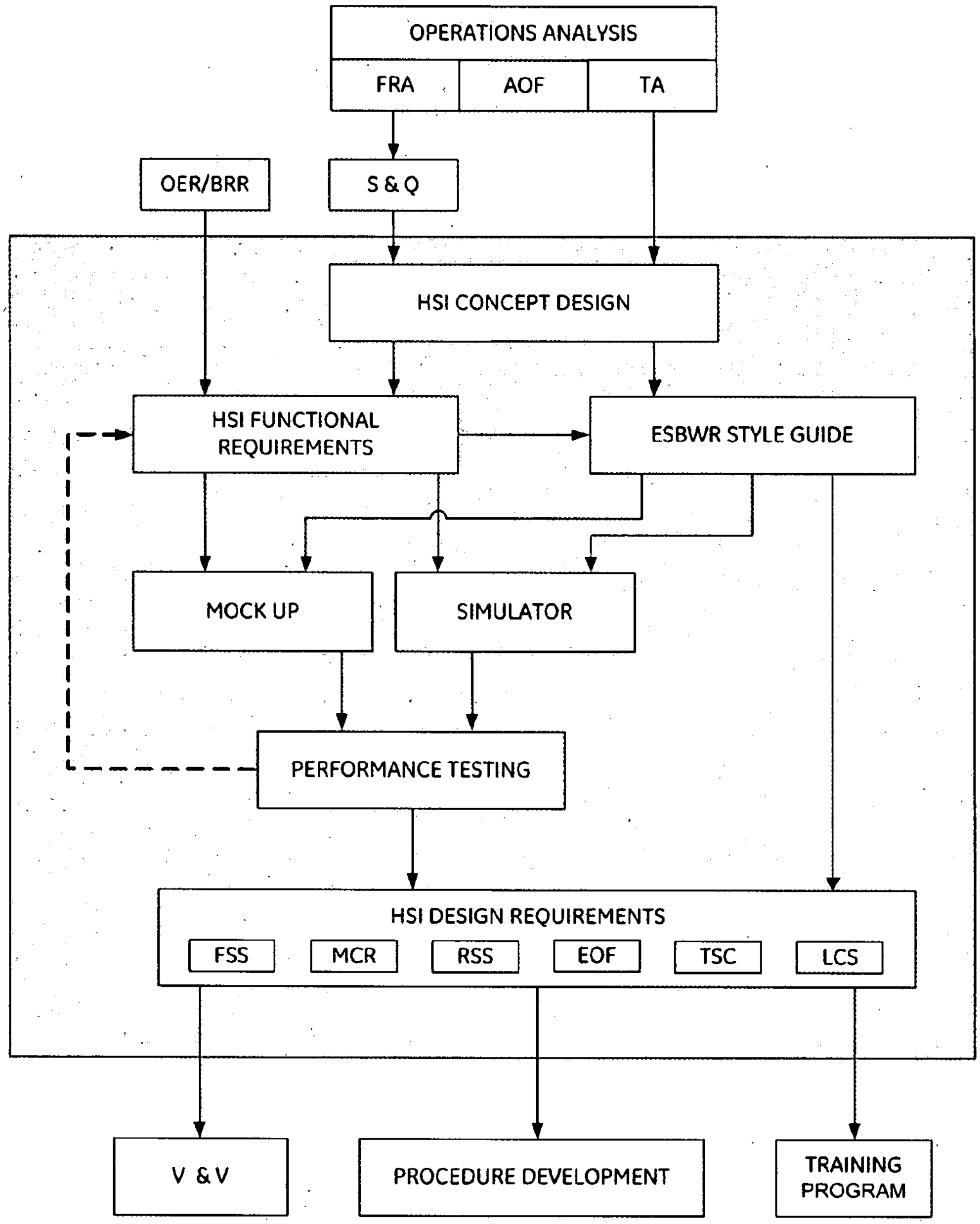

Figure 2. Human-System Interface Design Implementation Process

APPENDIX A: HSI DEVELOPMENT WORK PROCESS

NOTES:

[[

]]

A.1 DEVELOP A CONCEPT OF OPERATIONS

[[

]]

A.2 OBTAIN DESIGN INPUTS

[[

]]

A.3 HSI CONTROL ROOM CONCEPT DESIGN

[[

]]

A.4 HSI CONTROL ROOM CONCEPT PANEL PLACEMENT

[[

]]

A.5 HSI DETAILED DESIGN AND HARDWARE INTEGRATION

[[

]]

A.6 HSI DETAILED DESIGN AND HARDWARE INTEGRATION

[[

]]

A.7 HSI SCREEN FUNCTIONAL REQUIREMENTS CONCEPT DESIGN

[[

]]

A.8 HSI SCREEN FUNCTIONAL REQUIREMENTS DETAILED DESIGN AND INTEGRATION

[[

]]

[[

]]

Figure A-1. Type of Information and Specificity Contained in the ESBWR Style Guide Sheet 1 of 2

[[

]]

Figure A-1. Type of Information and Specificity Contained in the ESBWR Style Guide Sheet 2 of 2

APPENDIX B:HSI TEST AND EVALUATION WORK PROCESS

[[

]]

B.1 EVALUATION GOAL ESTABLISHMENT

[[

]]

B.2 TRADE OFF EVALUATION OPTION

[[

]]

B.3 PERFORMANCE BASED EVALUATION OPTION

[[

]]

[[

]]

Figure B-1. HFE Evaluation Request Form
Sheet 1 of 2

[[

]]

Figure B-1. HFE Evaluation Request Form

Sheet 2 of 2

[[

]]

Figure B-2. Trade off Study Key Criteria Example List

[[ ]]

Figure B-3. Pugh Matrix

[[

]]

Figure B-4. HFE Performance Test Methods and Measures

Sheet 1 of 2

[[

]]

Figure B-4. HFE Performance Test Methods and Measures
Sheet 2 of 2

[[

			]]

Figure B-5. Evaluation/Observation Form

[[

...	...	...	...	...
...	...	...	...	...
...	...	...	...	...
...	...	...	...	...
...	...	...	...	...
...	...	...	...	...
...	...	...	...	...
...	...	...	...	...
...	...	...	...	...

]]

Figure B-6. Usability Questionnaire
Sheet 1 of 2

[[

]]

Figure B-6. Usability Questionnaire
Sheet 2 of 2

[[

]]

Figure B-7. Modified Cooper Harper Workload Assessment

MFN 09-352

Enclosure 3

Licensing Topical Report NEDE-33268P

"ESBWR Human Factors Engineering Human-System Interface Design Implementation Plan"

Revision 4

Affidavit

GE-Hitachi Nuclear Energy Americas LLC

AFFIDAVIT

I, Larry J. Tucker, state as follows:

(1) I am Manager, ESBWR Engineering, GE Hitachi Nuclear Energy ("GEH"), and have been delegated the function of reviewing the information described in paragraph (2) which is sought to be withheld, and have been authorized to apply for its withholding.

(2) The information sought to be withheld is contained in enclosure 1 of GEH's letter, MFN 09-352 Mr. Richard E. Kingston to U.S. Nuclear Energy Commission, entitled "Submittal of Licensing Topical Report NEDE-33268P, ESBWR Human Factors Engineering Human-System Interface Design Implementation Plan, Revision 4," dated May 26, 2009. The proprietary information in enclosure 1, which is entitled "*MFN 09-352– Licensing Topical Report NEDE-33268P, ESBWR Human Factors Engineering Human-System Interface Design Implementation Plan, Revision 4," – GEH Proprietary Information,*" is delineated by a [[dotted underline inside double square brackets[3]]]. Figures and large equation objects are identified with double square brackets before and after the object. In each case, the superscript notation [3] refers to Paragraph (3) of this affidavit, which provides the basis for the proprietary determination.

(3) In making this application for withholding of proprietary information of which it is the owner or licensee, GEH relies upon the exemption from disclosure set forth in the Freedom of Information Act ("FOIA"), 5 USC Sec. 552(b)(4), and the Trade Secrets Act, 18 USC Sec. 1905, and NRC regulations 10 CFR 9.17(a)(4), and 2.390(a)(4) for "trade secrets" (Exemption 4). The material for which exemption from disclosure is here sought also qualify under the narrower definition of "trade secret", within the meanings assigned to those terms for purposes of FOIA Exemption 4 in, respectively, Critical Mass Energy Project v. Nuclear Regulatory Commission, 975F2d871 (DC Cir. 1992), and Public Citizen Health Research Group v. FDA, 704F2d1280 (DC Cir. 1983).

(4) Some examples of categories of information which fit into the definition of proprietary information are:

a. Information that discloses a process, method, or apparatus, including supporting data and analyses, where prevention of its use by GEH's competitors without license from GEH constitutes a competitive economic advantage over other companies;

b. Information which, if used by a competitor, would reduce his expenditure of resources or improve his competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing of a similar product;

c. Information which reveals aspects of past, present, or future GEH customer-funded development plans and programs, resulting in potential products to GEH;

d. Information which discloses patentable subject matter for which it may be desirable to obtain patent protection.

The information sought to be withheld is considered to be proprietary for the reasons set forth in paragraphs (4)a. and (4)b. above.

(5) To address 10 CFR 2.390(b)(4), the information sought to be withheld is being submitted to NRC in confidence. The information is of a sort customarily held in confidence by GEH, and is in fact so held. The information sought to be withheld has, to the best of my knowledge and belief, consistently been held in confidence by GEH, no public disclosure has been made, and it is not available in public sources. All disclosures to third parties, including any required transmittals to NRC, have been made, or must be made, pursuant to regulatory provisions or proprietary agreements which provide for maintenance of the information in confidence. Its initial designation as proprietary information, and the subsequent steps taken to prevent its unauthorized disclosure, are as set forth in paragraphs (6) and (7) following.

(6) Initial approval of proprietary treatment of a document is made by the manager of the originating component, the person most likely to be acquainted with the value and sensitivity of the information in relation to industry knowledge, or subject to the terms under which it was licensed to GEH. Access to such documents within GEH is limited on a "need to know" basis.

(7) The procedure for approval of external release of such a document typically requires review by the staff manager, project manager, principal scientist, or other equivalent authority for technical content, competitive effect, and determination of the accuracy of the proprietary designation. Disclosures outside GEH are limited to regulatory bodies, customers, and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and then only in accordance with appropriate regulatory provisions or proprietary agreements.

(8) The information identified in paragraph (2) is classified as proprietary because it contains details of GEH's design and licensing methodology. The development of the methods used in these analyses, along with the testing, development and approval of the supporting methodology was achieved at a significant cost to GEH.

(9) Public disclosure of the information sought to be withheld is likely to cause substantial harm to GEH's competitive position and foreclose or reduce the availability of profit-making opportunities. The information is part of GEH's comprehensive BWR safety and technology base, and its commercial value extends beyond the original development cost. The value of the technology base goes beyond the extensive physical database and analytical methodology and includes development of the expertise to determine and apply the appropriate

evaluation process. In addition, the technology base includes the value derived from providing analyses done with NRC-approved methods.

The research, development, engineering, analytical and NRC review costs comprise a substantial investment of time and money by GEH.

The precise value of the expertise to devise an evaluation process and apply the correct analytical methodology is difficult to quantify, but it clearly is substantial.

GEH's competitive advantage will be lost if its competitors are able to use the results of the GEH experience to normalize or verify their own process or if they are able to claim an equivalent understanding by demonstrating that they can arrive at the same or similar conclusions.

The value of this information to GEH would be lost if the information were disclosed to the public. Making such information available to competitors without their having been required to undertake a similar expenditure of resources would unfairly provide competitors with a windfall, and deprive GEH of the opportunity to exercise its competitive advantage to seek an adequate return on its large investment in developing and obtaining these very valuable analytical tools.

I declare under penalty of perjury that the foregoing affidavit and the matters stated therein are true and correct to the best of my knowledge, information, and belief.

Executed on this 26th day of May 2009.

Larry J. Tucker

Larry J. Tucker
GE-Hitachi Nuclear Energy Americas LLC